(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
G06F 15/00

(11) 공개번호 특2002 -0063659
(43) 공개일자 2002년08월05일

(21) 출원번호 10 -2001 -0004215
(22) 출원일자 2001년01월30일

(71) 출원인 주식회사 디지캡
서울특별시 서초구 서초3동 1708 -7 영인빌딩 3,4층

(72) 발명자 신용태
서울특별시강남구압구정동현대아파트20동1001호

(74) 대리인 최이욱

심사청구 : 없음

(54) 디지털 컨텐츠 복제 방지 장치 및 방법

요약

본 발명은 클라이언트에게 제공되는 디지털 컨텐츠의 불법 복제를 효과적으로 차단하기 위한 디지털 컨텐츠 복제 방지 장치 및 방법에 관한 것이다. 본 발명의 인증 서버는 네트워크를 통해 접속된 클라이언트의 사용자 정보 및 디지털 컨텐츠 제공 서버의 정보에 의해 서비스 등록키를 인증서버에 의해 생성하고, 클라이언트 단말기의 시스템 정보에 의해 암호화된 디지털 컨텐츠 파일을 복호화하기 위한 사용자 권한키를 생성한다. 디지털 컨텐츠 제공 서버는 서비스 등록키를 다단계 암호화하여 파일 암호화키를 생성함에 의해 디지털 컨텐츠 파일을 암호화하여 클라이언트에게 제공한다. 클라이언트는 사용자 권한키를 다단계 암호화 및 복호화하여 파일 복호화키를 생성하여 암호화된 디지털 컨텐츠 파일을 복호화한다. 또한, 본 발명은 서비스 등록키, 파일 암호화키 및 파일 복호화키 생성을 위해 투피시 알고리즘이 사용된다.

대표도
도 1

색인어
디지털 컨텐츠, 인증 서버, 복제, 시스템 정보, 파일 암호화키, 파일 복호화키, 투피시 알고리즘

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 디지털 컨텐츠 불법 복제 방지 장치의 구성 블록도.

도 2는 클라이언트의 서비스 등록을 위한 개략적 흐름 구성도.

도 3은 투피시 블록 암호화기의 개략적 구성도.

도 4는 클라이언트의 서비스 등록 취소를 위한 개략적 흐름 구성도.

도 5는 클라이언트의 디지털 컨텐츠 파일을 제공받기 위한 개략적 흐름 구성도.

도 6은 암호화된 디지털 컨텐츠 파일의 헤더 구성을 나타낸 도면.

도 7은 본 발명에 따른 디지털 컨텐츠 복제 방지를 수행하기 위한 플로우 챠트.

도 8은 디지털 컨텐츠 파일 암호화를 위한 파일 암호화키 생성을 수행하기 위한 플로우 챠트.

도 9는 인증 서버에 의한 사용자 권한 정보 생성을 수행하기 위한 플로우 챠트.

도 10은 본 발명에 따른 디지털 컨텐츠 파일의 복호화를 수행하기 위한 플로우 챠트.

< 도면의 주요부분에 대한 부호의 설명 >

100 : 인증 서버

102 : 디지털 컨텐츠 제공 서버

104 : 클라이언트

106 :클라이언트 정보 데이터베이스

108 : 디지털 컨텐츠 정보 데이터베이스

110 : 인증 정보 데이터베이스

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 디지털 컨텐츠 복제 방지 장치 및 방법에 관한 것으로서, 보다 상세하게는 클라이언트에게 제공되는 디지털 컨텐츠의 불법 복제를 효과적으로 차단하기 위한 디지털 컨텐츠 복제 방지 장치 및 방법에 관한 것이다.

현대인들은 방송, 출판 등과 같은 각종 미디어를 통해 제공되는 정보의 홍수 속에서 살고 있다. 각종 미디어를 통해 제공되는 정보를 통합하여 한꺼번에 공급하고자 하는 정보 공급자가 생겨났으며, 정보 공급자에 의해 공급되는 디지털 컨텐츠 중 원하는 컨텐츠만을 선택적으로 제공받고자 하는 사용자가 생기게 되었다.

이에 따라 각종 정보를 디지털 컨텐츠로 변환한 후 이 디지털 컨텐츠를 각각의 사용자에게 공급한 수 있도록 저장하는 정보 공급자와, 네트워크를 통해 정보 공급자로부터 디지털 컨텐츠를 제공받는 사용자로 이루어진 디지털 컨텐츠 전송 시스템들이 출현하게 되었다.

이와 같은, 디지털 컨텐츠 전송 시스템은 사용자에게 디지털 컨텐츠를 손쉽게 다운로드(download)받을 수 있는 응용 프로그램을 공급하였다.

또한, 네트워크에 의해 디지털 컨텐츠 전송 시스템과 접속된 사용자는 다운로드된 응용 프로그램을 통해 원하고자 하는 모든 정보를 얻을 수 있게 되었다.

이러한, 디지털 컨텐츠 전송 시스템에서 공급하고 있는 디지털 컨텐츠는 무료 또는 유료로 사용자에게 공급된다.

유료로 공급되는 디지털 컨텐츠는 디지털 컨텐츠 전송 시스템에 의해 각각의 서비스 요금이 정해진다.

이렇게 서비스 요금이 정해진 디지털 컨텐츠를 사용자가 전송받게 되면 서비스 서버는 사용자의 정보 이용량에 따라 서비스 요금을 누적시켜 사용자에게 부과한다.

그러나, 네트워크를 이용하여 상업적으로 디지털 컨텐츠를 제공하는 시스템에 사용자가 접속해서 유료용 디지털 컨텐츠를 전송받는 경우, 대부분의 사용자가 복제 형식으로 다른 사람에게 유료용 디지털 컨텐츠를 무단으로 배포하는 문제점이 있다.

또한, 복제된 디지털 컨텐츠에 의한 사용에 대한 공급자의 피해가 심각하나 이를 근본적으로 방지할 수 없는 문제점도 있다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명은 종래 기술의 제반 문제점을 해결하기 위하여 안출한 것으로서, 다단계의 암호화를 통해 생성된 파일 암호화키에 의해 디지털 컨텐츠 파일을 암호화하기 위한 디지털 컨텐츠 복제 방지 장치 및 방법을 제공함에 그 목적이 있다.

또한, 본 발명의 다른 목적은 암호화된 디지털 컨텐츠 파일을 복호화하기 위한 사용자 권한키를 클라이언트 단말기의 시스템 정보에 의해 생성하기 위한 디지털 컨텐츠 복제 장치 및 방법을 제공함에 있다.

발명의 구성 및 작용

상술한 목적들을 달성하기 위한 본 발명의 인증 서버는 네트워크를 통해 접속된 클라이언트의 사용자 정보 및 디지털 컨텐츠 제공 서버의 정보에 의해 서비스 등록키를 인증서버에 의해 생성하고, 클라이언트 단말기의 시스템 정보에 의해 암호화된 디지털 컨텐츠 파일을 복호화하기 위한 사용자 권한키를 생성한다.

디지털 컨텐츠 제공 서버는 서비스 등록키를 다단계 암호화하여 파일 암호화키를 생성함에 의해 디지털 컨텐츠 파일을 암호화하여 클라이언트에게 제공한다.

또한, 클라이언트는 사용자 권한키를 다단계 암호화 및 복호화하여 파일 복호화키를 생성하여 암호화된 디지털 컨텐츠 파일을 복호화함에 특징이 있다.

또한, 본 발명은 서비스 등록키, 파일 암호화키 및 파일 복호화키 생성을 위해 투피시 알고리즘이 사용된다.

이하, 본 발명에 따른 디지털 콘텐츠 불법 복제 방지 장치 및 방법을 바람직한 일 실시예를 참조하여 상세히 설명한다.

도 1은 본 발명에 따른 디지털 컨텐츠 불법 복제 방지 장치의 구성 블록도이고, 도 2는 클라이언트의 서비스 등록을 위한 개략적 흐름 구성도이며, 도 3은 투피시 블록 암호화기의 개략적 구성도이다.

도 4는 클라이언트의 서비스 등록 취소를 위한 개략적 흐름 구성도이고, 도 5는 클라이언트의 디지털 컨텐츠 파일을 제공받기 위한 개략적 흐름 구성도이며, 도 6은 암호화된 디지털 컨텐츠 파일의 헤더 구성을 나타낸 도면이다.

도 1에 도시된 바와 같이, 본 발명은 인증 서버(100), 디지털 컨텐츠 제공 서버(102), 클라이언트(104), 클라이언트 정보 데이터베이스(106), 디지털 컨텐츠 정보 데이터베이스(108) 및 인증 정보 데이터베이스(110)를 포함하여 구성된다.

여기서, 인증 서버(100)는 디지털 컨텐츠 제공 서버(102)를 통해 제공되는 디지털 컨텐츠 파일의 암호화 및 클라이언트(104)의 파일 사용 권한 정보 생성을 위한 시드키(Seed key)(Cap ID)를 생성하도록 구성된다.

여기서, 시드키(Cap ID)는 디지털 컨텐츠 정보를 제공받거나 또는 암호화된 디지털 컨텐츠를 복호화하기 위한 서비스를 제공받기 위한 서비스 등록키이다.

또한, 인증 서버(100)는 암호화된 디지털 컨텐츠 파일을 복호화하기 위해 일정 암호화 알고리즘에 의해 시드키(Cap ID) 및 클라이언트(104)의 시스템 정보를 암호화하여 디지털 컨텐츠 파일의 사용 권한키(이하, 토큰이라 칭함)를 생성하고, 생성된 토큰을 클라이언트(104)로 전송하도록 구성된다.

여기서, 토큰 생성을 위한 클라이언트(104)의 시스템 정보는 CPU의 크기, 개수 및 하드디스크의 페이지 크기 정보 등이 포함하여 구성된다. 또한, 토큰 생성을 위한 암호화 알고리즘은 투피시(twofish)이다.

디지털 컨텐츠 제공 서버(102)는 투피시 알고리즘을 이용하여 인증 서버(100)로부터 전송된 시드키(Cap ID)를 4단계의 암호화를 통해 파일 암호화키(FKey1)를 생성하도록 구성된다.

클라이언트(104)는 인증 서버(100)로부터 전송된 토큰을 단말기 내부의 저장 영역인 레지스트리에 저장하고, 토큰 및 디지털 컨텐츠 제공 서버(102)로부터 다운로딩된 암호화된 디지털 컨텐츠 파일 헤더 정보에 따른 암호화 및 복호화를 통해 파일 암호화키(FKey1)에 상응하는 파일 복호화키(FKey2)를 생성하여 암호화된 디지털 컨텐츠 파일을 복호화하도록 구성된다.

여기서, 본 발명은 파일 암호화키(FKey1) 생성시 키의 암호화 및 복호화를 위해 투 피시 알고리즘을 사용한다.

클라이언트 정보 데이터베이스(106)는 클라이언트(104)의 사용자 정보 및 해당 시드키(Cap ID)를 저장하고, 디지털 컨텐츠 정보 데이터베이스(108)는 파일 ID에 따라 분류된 해당 디지털 컨텐츠 정보가 저장되도록 구성된다.

또한, 인증 정보 데이터베이스(110)는 클라이언트(104)의 해당 서비스 등록키 즉, 시드키(Cap ID)를 저장하도록 구성된다.

이와 같이 구성되는 본 발명에 따른 디지털 컨텐츠 복제 방지 장치의 동작을 첨부 도면을 참조하여 설명하면 다음과 같다.

먼저, 디지털 컨텐츠 제공 서버(102)로부터의 디지털 컨텐츠 파일을 제공받기 위한 클라이언트(104)의 서비스 등록 과정을 도 2를 참조하여 설명한다.

클라이언트(104)는 디지털 컨텐츠 제공 서버(102)로부터 전송되는 디지털 컨텐츠 파일을 실행시키기 위한 디지털 컨텐츠 실행 프로그램을 다운로딩하고, 다운로딩된 실행 프로그램을 실행시킴에 따라 디지털 컨텐츠 실행 프로그램을 설치한다.

이때, 디지털 컨텐츠 실행 프로그램의 다운로딩은 서비스 등록 과정 내에 포함되어 실행될 수 있을 뿐만 아니라 서비스 등록 이전에 미리 다운로딩되어 설치될 수 있음은 자명하다.

여기서, 디지털 컨텐츠 실행 프로그램은 MP3 플레이어, 미디어 플레이어 또는 리얼 플레이어 등이 있다.

이어, 클라이언트(104)는 네트워크 예를 들어, 인터넷 접속을 통해 디지털 컨텐츠 제공 서버(102)에 접속하고, 사용자 정보를 입력하여(단계 200) 서비스 등록을 요청한다(단계 202).

여기서, 사용자 정보는 적어도 클라이언트(104)의 성명, ID, 패스워드 및 주민등록번호를 포함한다.

디지털 컨텐츠 제공 서버(102)는 클라이언트(104)로부터 입력되는 사용자 정보를 클라이언트 정보 데이터베이스(106)에 저장하고, 그 중 주민등록번호, 클라이언트 성명(또는 ID) 및 패스워드와 디지털 컨텐츠 제공 서버 번호(SP_NO)를 인증 서버(100)로 전송함에 따라 인증 사용자 등록을 요청한다(단계 204).

여기서, 디지털 컨텐츠 제공 서버 번호(SP_NO)는 인증 서버(100)에 네트워크 접속된 디지털 컨텐츠 제공 서버가 복수개 존재하는 경우 이를 구별하기 위한 정보이다.

인증 서버(100)는 디지털 컨텐츠 제공 서버(102)로부터 요청된 인증 사용자 등록을 위해 시드키(Cap ID)를 생성한다.

즉, 인증 서버(100)는 수학식 1에서와 같이, 디지털 컨텐츠 제공 서버(102)로부터 전송된 서비스 제공 서버 번호(SP_NO), 주민등록번호 및 클라이언트의 성명 를 투피시 알고리즘에 따른 제1 설정키(auLKey)에 의해 암호화를 수행하여 시드키(Cap ID)를 생성한다(단계 206).

여기서, 제1 설정키(auLKey)는 프로그램에 의해 미리 설정된 키값으로 설정될 수 있다.

수학식 1

$$\text{Cap ID} = E_{auLKey}[\text{SP\_NO}(4) \| \text{주민등록번호}(13) \| \text{클라이언트 성명}(30)]$$

이때, 괄호 안의 숫자는 바이트(Byte) 단위를 나타내고, 미리 설정된 키 값(auLKey)은 암호화를 위해 프로그래머(programmer) 등에 의해 미리 정의된 값이며, E는 암호화(Encryption)의 약자이다.

여기서, 투피시 알고리즘은 데이터 암호화 표준(Data Encryption Standards)을 대체하기 위해 미국의 상무부 기술표준국(NIST)에서 발표한 ASE(Advanced Encryption Standard)에서 채택된 알고리즘이다.

투피시 알고리즘은 128비트(bits)의 대칭형 블록 암호기이고, 128비트, 192비트 및 256 비트 등의 다양한 키 길이를 가지며, 다양한 소프트웨어 및 하드웨어의 플랫폼에 효율적이다.

또한, 투피시 블록 암호화기의 구조는 도 3에 도시된 바와 같이, 전단사 기능의 에프 함수와 함께 하는 16순환 페이스텔(feistel) 망구조를 갖고, 입출력부에 부가 화이테닝부(whitening)를 가진다.

여기서, 페이스텔 망은 복수개의 에스 -박스(S -box), 엠디에스(MDS) 행렬 및 피에이치티(PHT)를 포함하여 구성된다.

이와 같은 구성을 갖는 투피시 블록 암호화기에 따른 암호문 생성 과정을 개략적으로 설명한다.

원문서는 4r의 32 비트 단어로 나누어지고, 입력 화이테닝 단계에서 이들 4개이 키 단어와 배타 논리합을 한다. 이후에 16번의 순환이 순차적으로 수행되는데, 각 라운드에서는 왼쪽의 두 개의 단어는 투피시의 가장 중요한 부분인 g함수의 입력으로 사용된다.

g 함수는 4개의 바이트 와이드 키 독립 에스 박스로 구성되며, 이후 엠디에스 행렬에 근간하는 하나의 선형 혼합 단계가 수행된다. 두 개의 g 함수의 결과는 피에이치티를 사용하여 조합되고, 두 개의 키워드가 더해진다.

이 두 개의 결과는 배타적 논리합이 되어 오른쪽 단어(먼저, 그들 중 하나는 1비트 왼쪽으로 회전하고, 그 후에 다른 것은 오른쪽으로 회전한다)와 배타 논리합이 된다.

이어, 다음 처리 단계를 위해서 왼쪽 반쪽과 오른쪽 반쪽이 바뀌고, 모든 처리 단계 이후 마지막 처리 단계는 바꿈이 반대로 되어진다.

그리고, 4개의 단어는 암호문을 생성하기 위해 4개 이상의 키 단어와 배타적 논리합이 수행된다.

인증 서버(100)는 상술한 바와 같은 동작을 수행하는 투피시 알고리즘에 의해 생성된 시드키(Cap ID)와 사용자 인증 등록 완료 메시지를 생성하여(단계 208) 디지털 컨텐츠 제공 서버(102)로 전송한다(단계 210).

디지털 컨텐츠 제공 서버(102)는 인증 서버(100)로부터의 시드키(Cap ID)를 클라이언트 정보 데이터베이스(106)에 저장한 후(단계 212), 서비스 등록 완료 메시지를 생성하여(단계 214) 클라이언트(104)에게 전송한다(단계 216).

이어, 도 4를 참조하여 클라이언트(104)의 서비스 등록 취소 요청에 따른 동작을 설명한다.

먼저, 클라이언트(104)가 사용자 정보 즉, 주민등록번호 및 패스워드를 입력하고(단계 400), 서비스 등록 요청 신호를 디지털 컨텐츠 제공 서버(102)로 전송한다(단계 402).

디지털 컨텐츠 제공 서버(102)는 클라이언트(104)로부터의 주민등록번호 및 패스워드와 클라이언트 정보 데이터베이스(106)에 저장되어 있는 클라이언트 정보를 비교하여 클라이언트(104)가 서비스 등록자인지를 판단한다(단계 404).

클라이언트(104)가 서비스 등록자인 경우, 디지털 컨텐츠 제공 서버(102)는 클라이언트(104)의 해당 시드키(Cap ID)를 검색하고, 디지털 컨텐츠 제공 서버 번호(SP_NO), 주민등록번호 및 시드키(Cap ID)를 인증 서버(100)로 전송함에 따라(단계 406) 사용자 인증 취소를 요청한다(단계 408).

인증 서버(100)는 디지털 컨텐츠 제공 서버(102)로부터의 사용자 인증 취소 요청신호에 따라 인증 정보 데이터베이스(110)를 검색하여 클라이언트(104)가 인증 사용자인지를 판단한다(단계 410).

클라이언트(104)가 인증 사용자인 경우, 인증 서버(100)는 클라이언트(104)의 사용자 인증 정보를 삭제함에 따라 사용자 인증 취소를 수행하고(단계 412), 사용자 인증 취소 완료 메시지를 생성하여 디지털 컨텐츠 제공 서버(102)로 전송한다(단계 414).

디지털 컨텐츠 제공 서버(102)는 인증 서버(100)로부터의 사용자 인증 취소 완료 메시지에 따라 서비스 등록 취소 완료 메시지를 생성하고(단계 418), 생성된 서비스 등록 취소 완료 메시지를 클라이언트(104)에세 전송함에 따라 클라이언트(104) 의 서비스 등록 취소가 완료된다(단계 420).

이어, 서비스 등록이 완료된 클라이언트(104)가 디지털 컨텐츠 제공 서버(102)로부터의 디지털 컨텐츠 파일을 제공받아 실행하는 동작을 도 5를 참조하여 설명한다.

먼저, 클라이언트(104)는 네트워크를 통해 디지털 컨텐츠 제공 서버(102)에 접속한 후 ID 및 패스워드 입력 등에 따른 로그인을 수행한 후 제공되는 다양한 디지털 컨텐츠 파일 중 어느 하나를 선택하는 파일 요청 신호를 입력한다(단계 500).

디지털 컨텐츠 제공 서버(102)는 클라이언트(104)로부터 입력되는 ID 및 패스워드를 클라이언트 정보 데이터베이스(106)에 저장되어 있는 해당 정보와 비교함에 따라 서비스 등록 여부를 판단한다(단계 502).

클라이언트(104)가 서비스 등록자인 경우, 디지털 컨텐츠 제공 서버(102)는 클라이언트(104)가 요청한 해당 디지털 컨텐츠 파일을 암호화하기 위한 파일키(FKey1)를 생성한다(단계 504).

즉, 디지털 컨텐츠 제공 서버(102)는 파일 암호화키(FKey1) 생성을 위해 시드키(Cap ID) 및 클라이언트의 사용자 정보 등을 투피시 알고리즘에 의해 다단계 암호화를 수행하는데, 이를 상세히 설명하면 다음과 같다.

먼저, 디지털 컨텐츠 제공 서버(102)는 클라이언트 정보 데이터베이스(106)에 저장되어 있는 클라이언트(104)의 해당 시드키(Cap ID)를 제2 설정키(asUkey)을 이용하여 암호화함에 따라 제1 파일 암호화키(DasUKey1)를 생성한다.

이때, 제2 설정키(asUkey)는 시드키(Cap ID) 생성시의 제1 설정키(auLKey)와 동일하도록 구성되거나 또는 다르게 구성될 수 있다.

이어, 디지털 컨텐츠 제공 서버(102)는 수학식 2에서와 같이, 생성된 제1 파일 암호화키(DasUKey1)를 이용하여 디지털 컨텐츠 제공 서버 번호(SP_NO), 주민등록번호 및 시드키(Cap ID)의 스트림을 암호화하여 파일 암호화키(FKey1) 생성을 위한 초기 암호화키인 제2 파일 암호화키(UKey1)를 생성한다.

수학식 2

$$UKey1 = E_{DasUKey1} \quad [SP\_NO(4) \parallel 주민등록번호(13) \parallel Cap\ ID(16)]$$

여기서, E는 암호화의 약자를 의미하고, 암호화를 위한 알고리즘은 투피시 알고리즘이며, 괄호안의 숫자는 바이트 숫자를 나타낸다.

또한, 디지털 컨텐츠 제공 서버(102)는 미리 설정된 키 값(auPKey)에 따라 디지털 컨텐츠 제공 서버(102)의 랜덤값을 암호화하여 제3 파일 암호화키(DauFKey1)를 생성한다.

여기서, 디지털 컨텐츠 서비스 서버의 랜덤값은 일정의 프로그램에 의해 무작위로 형성된 값으로 16바이트로 구성된다.

이어, 디지털 컨텐츠 제공 서버(102)는 수학식 3에서와 같이, 제2 파일 암호화키(UKey1), 선택된 디지털 컨텐츠 파일 ID 및 디지털 컨텐츠 제공 서버 랜덤값을 제3 파일 암호화키(DauFKey1)를 이용하여 암호화함에 따라 파일 암호화키(FKey1)를 생성한다.

수학식 3

$$FKey1 = E_{DauFKey1} \quad [UKey1(16) \parallel 파일\_ID(8) \parallel 디지털\ 컨텐츠\ 제공\ 서버\ 랜덤(8)]$$

여기서, 괄호안의 숫자는 바이트 단위, 디지털 컨텐츠 제공 서버 랜덤값은 일정 프로그램에 의해 무작위로 형성된 값이며, E는 암호화의 약자를 나타낸다.

디지털 컨텐츠 제공 서버(102)는 다단계의 암호화를 통해 생성된 파일 암호화키(FKey1)에 의해 클라이언트(104)로부터 요청된 디지털 컨텐츠 파일을 암호화하여 클라이언트(104)에게 전송한다.

이때, 암호화되어 클라이언트(104)에게 전송되는 디지털 컨텐츠 파일은 도 6에 도시된 바와 같은 구성의 헤더를 갖는다.

도 6을 참조하면, 디지털 컨텐츠 파일의 헤더 정보는 디지털 컨텐츠 제공 서버 번호 필드(600), 파일 설명 필드(602), 파일 타입 필드(604), 파일 ID 필드(606), 클라이언트(104) 성명 필드(608), 제1 예비 영역(flag) 필드(610), 암호화될 파일의 총 사이즈 필드(612), 헤더, 바디 및 확장 영역을 포함하는 디지털 컨텐츠 파일의 총 사이즈 필드(614), 암호화된 파일의 총 사이즈 필드(616), 에러 검출을 위한 암호화될 파일의 체크섬(checksum) 필드(618), 제2 예비 영역 필드(620), 서비스 서버 랜덤 필드(622), 파일 암호화키 확인값(KVC) 필드(624), 제3 예비 영역 필드(626) 및 파일 헤더의 에러 검출을 위한 체크섬 필드(628)로 구성된다.

여기서, 파일 암호화키 확인값 필드(624)의 확인값(KVC)은 16 바이트의 널(Null)을 이전의 파일 암호화키에 의해 암호화하여 생성되는데, 디지털 컨텐츠 제공 서버(102)는 파일 암호화를 위해 생성된 파일 암호화키(FKey1)와 확인값(KVC)을 비교함에 따라 생성된 파일 암호화키(FKey1)의 정상 여부를 확인한다.

클라이언트(104)는 상술한 바와 같은 구성을 갖는 헤더가 포함된 디지털 컨텐츠 파일을 다운로딩하고, 디지털 컨텐츠 파일을 실행하기 위한 복호화를 수행한다.

즉, 클라이언트(104)는 다운로딩된 디지털 컨텐츠 파일의 복호화키 생성을 위하여 시스템 정보를 추출하고, 추출된 시스템 정보를 포함하는 토큰 요청 신호를 전송한다.

또한, 시스템 정보는 토큰을 요청한 클라이언트 시스템이 가지는 정보로서, CPU의 종류, 개수 및 하드디스크의 페이지 사이즈 등의 정보를 포함한다.

인증 서버(100)는 수학식 4에서와 같이, 클라이언트(104)로부터 전송된 서비스 제공 서버 번호, 주민등록번호 및 시스템 정보를 제1 설정키값(auLKey)에 의해 암호화하여 제1 토큰키(LKey1)를 생성한다.

수학식 4

$$LKey1 = E_{auLKey} \quad [\text{시스템 정보}(16)]$$

여기서, E는 암호화의 약자이고, 암호화를 위해 사용된 알고리즘은 투피시 알고리즘이며, 괄호안의 숫자는 바이트를 나타낸다.

인증 서버(100)는 생성된 제1 토큰키(LKey1)를 사용하여 16바이트의 인증 서버(100) 랜덤값을 암호화하여 제2 토큰키(SLKey1)를 생성한다. 이때, 인증 서버(100)는 16바이트의 널(Null)을 이전의 제2 토큰키에 의해 암호화함에 의해 생성된 확인키 값과 생성된 제2 토큰키(SLKey1)를 비교함에 따라 정상 여부를 확인한다.

여기서, 인증 서버(100) 랜덤값은 인증 서버(100)에서 일정 프로그램에 의해 무작위로 형성된 값이다.

인증 서버(100)는 제2 토큰키(SLKey1)를 이용하여 클라이언트(104)의 시드키(Cap ID)에 의해 생성된 16바이트의 제2 파일 암호화키(UKey1)를 암호화하여 제3 토큰키(EncUKey1)를 생성한다.

여기서, 제2 파일 암호화키(UKey1)는 디지털 컨텐츠 제공 서버(102)에서의 생성 과정이 동일하므로 그에 대한 상세한 설명은 생략하기로 한다.

인증 서버(100)는 제3 토큰키(EncUKey1)에 16바이트의 인증 서버 랜덤값을 부가한 [디지털 컨텐츠 암호화 서버 랜덤(16) ‖ 제3 토큰(16)] 형태로 구성한 토큰을 클라이언트(104)에게 전송한다.

이때, 토큰은 다운로딩되어 단말기의 저장 영역에 저장되는데, 토큰의 다운로딩 횟수를 제한적으로 구성할 수 있다.

클라이언트(104)는 단말기의 시스템 정보를 추출하고, 추출된 시스템 정보를 미리 설정된 키값(auLKey)에 의해 암호화하여 제1 복호화키(LKey2)를 생성한다.

또한, 클라이언트(104)는 토큰 내의 랜덤값을 제1 복호화키(LKey2)에 의해 암호화하여 제2 복호화키(SLKey2)를 생성한다.

여기서, 클라이언트(104)에 의해 생성되는 제1 복호화키(LKey2) 및 제2 복호화키(SLKey2)는 인증 서버(100)에서 생성되는 제1 토큰키(LKey1) 및 제2 토큰키(SLKey1)와 동일하고, 생성 과정도 동일하다.

클라이언트(104)는 제3 토큰키(EncUKey1)를 제2 복호화키(SLKey2)에 의해 복호화하여 제3 복호화키(UKey2)를 생성한다. 이때, 제3 복호화키(UKey2)는 제2 파일 암호화키(UKey1)와 동일한 키임은 자명하다.

또한, 클라이언트(104)는 암호화된 디지털 컨텐츠 파일 헤더로부터 추출한 서비스 제공 서버 랜덤을 제3 설정키(auFKey)에 의해 암호화하여 제4 파일키(DauFKey)를 생성한다.

이때, 제3 설정키(auFKey)는 제1 설정키(auLKey) 또는 제2 설정키(asUKey)와 동일하게 구성되거나 또는 다른 형태로 구성될 수 있다.

클라이언트(104)는 수학식 3에서와 같이, 암호화된 디지털 컨텐츠 파일로부터 추출된 파일 ID, 디지털 컨텐츠 제공 서버 랜덤 및 제3 복호화키(UKey2)를 제4 복호화키(DauFKey)에 의해 암호화함에 따라 파일 복호화키(FKey2)를 생성한다.

이때, 클라이언트(104)는 다운로딩된 디지털 컨텐츠 파일 헤더 내의 확인용키 값과 생성된 파일 복호화키(FKey2)를 비교함에 따라 정상 여부를 확인한다.

클라이언트(104)는 생성된 파일 복호화키(FKey2)를 이용하여 암호화된 디지털 컨텐츠 파일을 복호화하고, 실행 프로그램에 의해 디지털 컨텐츠 파일을 실행하게 된다.

여기서, 파일 복호화키(FKey2)는 디지털 컨텐츠 제공 서버(102)에서 디지털 컨텐츠 파일을 암호화한 파일 암호화키(FKey1)와 동일함은 자명하다.

이와 같이 구성되어 동작되는 본 발명에 따른 디지털 컨텐츠 복제 방지 장치의 수행 과정을 도 7을 참조하여 설명하면 다음과 같다.

도 7은 본 발명에 따른 디지털 컨텐츠 복제 방지를 수행하기 위한 플로우 챠트이다.

먼저, 디지털 컨텐츠 제공 서버(102)는 네트워크를 통해 접속된 클라이언트(104)로부터의 사용자 정보 입력 등에 따른 서비스 등록 요청 신호를 인증 서버로 전송하고, 인증 서버(100)는 사용자 정보에 따른 시드키를 생성하여 디지털 컨텐츠 제공 서버(102)로 전송한다(S700).

디지털 컨텐츠 제공 서버(102)는 시드키(Cap ID)를 다단계 암호화하여 파일 암호화키(FKey1)를 생성하고, 생성된 파일 암호화키(FKey1)에 의해 클라이언트(104)로부터 요청된 디지털 컨텐츠 파일을 암호화한다(S702).

이어, 인증 서버(100)는 클라이언트(104) 단말기의 시스템 정보를 다단계 암호화하여 생성된 사용자 권한키(토큰)를 클라이언트(104)로 전송한다(S704).

여기서, 시스템 정보는 클라이언트(104) 단말기만이 가지는 고유 정보로서, 시스템 정보에 의해 생성된 토큰은 클라이언트의 단말기마다 고유한 특징을 갖는다.

클라이언트(104)는 토큰을 이용하여 암호화 및 복호화에 의해 파일 복호화키(FKey2)를 생성하고, 생성된 파일 복호화키(FKey2)에 의해 암호화된 디지털 컨텐츠 파일을 복호화한다(S706).

이때, 시드키, 파일 암호화키, 토큰 및 파일 복호화키 생성을 위한 암호화 및 복호화시 이용되는 알고리즘은 투피시 알고리즘이다.

또한, 복호화된 디지털 컨텐츠 파일은 클라이언트(104) 단말기에 설치되어 있는 해당 실행 프로그램에 의해 실행된다.

이와 같이 구성되는 본 발명에 따른 디지털 컨텐츠 복제 방지 과정 중 파일 암호화키 생성 과정을 도 8을 참조하여 설명한다.

도 8은 디지털 컨텐츠 파일 암호화를 위한 파일 암호화키 생성을 수행하기 위한 플로우 챠트이다.

디지털 컨텐츠 제공 서버(102)는 인증 서버(100)로부터의 시드키를 미리 설정된 즉, 프로그래머 등에 의해 코드상에 하드 코딩된 키값을 이용하여 암호화함에 따라 제1 파일 암호화키(DasUKey1)를 생성한다(S800).

이어, 시드키, 클라이언트(104)의 주민등록번호 및 디지털 컨텐츠 제공 서버 번호를 제1 파일 암호화키(DasUKey1)에 의해 암호화하여 제2 파일 암호화키(UKey1)를 생성한다(S802).

일정 프로그램에 의해 무작위로 형성된 디지털 컨텐츠 제공 서버 랜덤값을 제2 파일 암호화키(UKey1)에 의해 암호화하여 제3 파일 암호화키(DauFKey1)를 생성한다(S804).

제2 파일 암호화키(UKey1), 클라이언트(104)로부터 요청된 디지털 컨텐츠 파일의 ID 및 랜덤값을 제3 파일 암호화키(DauFKey1)에 의해 암호화하여 파일 암호화키(FKey1)를 생성한다(S806).

이어, 널(Null) 함수를 이전의 파일 암호화키에 의해 암호화하여 형성된 파일 암호화키 확인용 키값(KVC)과 파일 암호화키(FKey1)를 비교하여 생성된 파일 암호화키(FKey1)의 정상 여부를 확인한다(S808).

정상 여부가 확인된 파일 암호화키(FKey1)에 의해 디지털 컨텐츠 파일을 암호화하여 클라이언트(104)로 전송한다(S810).

여기서, 제1 내지 제3 파일 암호화키 및 파일 암호화키 생성을 위한 암호화시 이용되는 알고리즘은 투피시 알고리즘이다.

또한, 도 7에서 사용자 권한 정보 즉, 토큰 생성을 위한 과정을 첨부 도면을 참조하여 보다 상세히 설명한다.

도 9는 인증 서버에 의한 사용자 권한 정보 생성을 수행하기 위한 플로우 챠트이다.

먼저, 인증 서버(100)는 클라이언트(104)로부터의 시스템 정보를 미리 설정된 키값(auLKey)에 의해 암호화하여 제1 토큰키(LKey1)를 생성하고(S900), 생성된 제1 토큰키(LKey1)에 의해 인증 서버(100)의 랜덤값을 암호화하여 제2 토큰키(SLKey1)를 생성한다(S902).

이어, 시드키(Cap ID)를 이용하여 생성된 제2 파일 암호화키(UKey1)를 제2 토큰키(SLKey1)에 의해 암호화하여 제3 토큰키(EncUKey1)를 생성한다(S904).

여기서, 제2 파일 암호화키(UKey1)는 도 8에서와 동일한 과정에 의해 생성되므로 상세한 설명을 생략하기로 한다.

인증 서버(100)는 생성된 제3 토큰키(EncUKey1)에 16바이트의 랜덤값을 부가한 형태의 토큰을 생성하여 클라이언트(104)로 전송한다(S906).

클라이언트에 의한 암호화된 디지털 컨텐츠 파일의 복호화 과정을 도 10을 참조하여 상세히 설명한다.

도 10은 본 발명에 따른 디지털 컨텐츠 파일의 복호화를 수행하기 위한 플로우 챠트이다.

클라이언트(104)는 단말기의 시스템 정보를 추출하고, 추출된 시스템 정보를 미리 설정된 키값(auLKey)에 의해 암호화하여 제1 복호화키(LKey2)를 생성한다(S1000).

이어, 인증 서버(100)로부터 전송되어 단말기의 일정 저장영역에 저장되어 있는 토큰 중 랜덤값을 제1 복호화키(LKey2)에 의해 암호화하여 제2 복호화키(SLKey2)를 생성한다(S1002).

토큰 중 제3 토큰키(EncUKey1)를 제2 복호화키(SLKey2)에 의해 복호화하여 제3 복호화키(UKey2)를 생성하고(S1004), 확인용 키값(KVC)과 생성된 제3 복호화키(UKey2)를 비교함에 따라 제3 복호화키(UKey2)의 정상 여부를 판단한다(S1006).

여기서, 확인용 키값(KVC)은 모든 바이트가 '0'으로 구성된 널(Null)을 이전의 제3 복호화키(UKey2)에 의해 암호화함에 생성된 키값이다.

위의 단계(S1004)에서 생성된 제3 복호화키(UKey2)에 의해 토큰 중 랜덤값을 암호화하여 제4 복호화키(DauFKey2)를 생성한다(S1008).

이어, 제3 복호화키(UKey2), 파일 ID 및 랜덤값을 제4 복호화키(DauFKey2)에 의해 암호화하여 파일 복호화키(FKey2)를 생성하고(S1010), 저장되어 있는 디지털 컨텐츠 파일 헤더의 확인용 키값(KVC)과 비교하여 파일 복호화키(FKey2)의 정상 여부를 확인한다(S1012).

정상 여부가 확인된 파일 복호화키(FKey2)에 의해 암호화된 디지털 컨텐츠 파일을 복호화하고, 단말기에 설치된 해당 실행 프로그램에 의해 디지털 컨텐츠 파일을 실행한다(S1014).

여기서, 제3 복호화키(UKey2)는 제2 파일 암호화키(FKey1)와 동일하고, 파일 복호화키(FKey2)와 파일 암호화키(FKey1)는 동일함을 자명하다.

발명의 효과

본 발명에 따른 디지털 컨텐츠 복제 방지 장치 및 방법은 디지털 컨텐츠를 암호화하기 위한 파일 암호화키, 디지털 컨텐츠 파일을 다운로드받거나 또는 다운로드된 디지털 컨텐츠 파일을 복호화하기 위한 사용자 권한 정보 및 파일 복호화키를 다단계의 암호화 과정을 통해 생성한다.

그러므로, 본 발명은 파일 암호화키, 사용자 권한 정보 및 파일 복호화키가 다단계의 암호화 과정을 통해 생성되므로 키의 해독이 거의 불가능하여 디지털 컨텐츠 파일의 복제를 방지할 수 있다.

또한, 사용자 권한 정보가 단말기의 시스템 정보를 포함하는 키값에 의해 생성되므로, 클라이언트의 단말기에 다운로드된 디지털 컨텐츠 파일을 다른 단말기로의 복제를 방지할 수 있는 효과도 있다.

(57) 청구의 범위

청구항 1.

네트워크를 통해 디지털 컨텐츠 제공 서버에 접속되는 인증 서버에 의한 디지털 컨텐츠 파일의 복제 방지 방법 -상기 디지털 컨텐츠 제공 서버는 암호화된 디지털 컨텐츠 파일을 클라이언트로 제공함 -에 있어서,

상기 클라이언트로부터의 사용자 정보에 따른 서비스 등록키를 생성하여 상기 디지털 컨텐츠 제공 서버로 전송하는 단계;

상기 클라이언트 단말기의 시스템 정보에 따른 사용자 권한키를 생성하여 상기 클라이언트로 전송하는 단계를 포함하되,

상기 디지털 컨텐츠 제공 서버는 상기 서비스 등록키를 다단계 암호화에 의한 파일 암호화키를 생성하여 상기 디지털 컨텐츠 파일을 암호화하고,

상기 클라이언트는 상기 사용자 권한키에 의한 다단계 암호화를 통해 상기 파일 암호화키에 상응하는 파일 복호화키를 생성하여 상기 암호화된 디지털 컨텐츠 파일을 복호화하는 것을 특징으로 하는 인증 서버에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 2.

제1항에 있어서,

상기 클라이언트로부터의 사용자 정보에 따른 서비스 등록키를 생성하여 상기 디지털 컨텐츠 제공 서버로 전송하는 단계는

상기 클라이언트의 사용자 정보를 상기 디지털 컨텐츠 제공 서버를 통해 입력받는 단계;

상기 사용자 정보 및 상기 디지털 컨텐츠 제공 서버의 정보를 일정의 암호화 알고리즘에 의해 암호화하여 상기 서비스 등록키를 생성하는 단계;

상기 사용자 정보 및 상기 디지털 컨텐츠 제공 서버 정보와 상기 서비스 등록키를 저장하는 단계;

상기 서비스 등록키를 상기 디지털 컨텐츠 제공 서버로 전송하는 단계

를 포함하는 인증 서버에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 3.

제1항 또는 제2항에 있어서,

상기 사용자 정보는 상기 클라이언트의 주민등록번호 및 성명 정보를 포함하는 것을 특징으로 하는 인증 서버에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 4.

제2항에 있어서,

상기 디지털 컨텐츠 제공 서버 정보는 상기 디지털 컨텐츠 제공 서버 번호 정보를 포함하는 것을 특징으로 하는 인증 서버에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 5.

제2항에 있어서,

상기 암호화 알고리즘은 투피시(twofish) 알고리즘임을 특징으로 하는 인증 서버에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 6.

제1항에 있어서,

상기 클라이언트 단말기의 시스템 정보에 따른 사용자 권한키를 생성하여 상기 클라이언트로 전송하는 단계는

상기 시스템 정보를 미리 설정된 키값에 의해 일정의 암호화 알고리즘을 적용하여 암호화함에 따른 제1 토큰키를 생성하는 단계;

상기 알고리즘을 사용하여 제1 토큰키에 의해 일정의 랜덤값을 암호화함에 따른 제2 토큰키를 생성하는 단계;

상기 알고리즘을 이용하여 상기 서비스 등록키를 암호화함에 의해 상기 디지털 컨텐츠 파일 암호화 초기키를 생성하는 단계;

상기 알고리즘을 이용하여 상기 생성된 파일 암호화 초기키를 상기 제2 토큰키에 의해 암호화하여 제3 토큰키를 생성하는 단계;

상기 제3 토큰키에 상기 랜덤값을 부가하여 사용자 권한키를 생성하는 단계;

상기 사용자 권한키를 상기 클라이언트로 전송하는 단계

를 포함하는 인증 서버에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 7.

제6항에 있어서,

상기 시스템 정보는 적어도 CPU의 종류, 개수 및 하드디스크의 페이지 사이즈 정보를 포함하는 것을 특징으로 하는 인증 서버에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 8.

제6항에 있어서,

상기 암호화 알고리즘은 투피시 알고리즘임을 특징으로 하는 인증 서버에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 9.

네트워크를 통해 디지털 컨텐츠 제공 서버에 접속된 클라이언트에 의한 디지털 컨텐츠 파일의 복제 방지 방법 -상기 디지털 컨텐츠 제공 서버는 네트워크를 통해 접속된 인증 서버로부터 서비스 등록키를 제공받고, 상기 디지털 컨텐츠 제공 서버는 상기 서비스 등록키의 다단계 암호화에 의해 생성된 파일 암호화키를 이용하여 상기 디지털 컨텐츠 파일을 암호화함 -에 있어서,

상기 인증 서버로 상기 클라이언트 단말기의 시스템 정보를 전송하는 단계;

상기 시스템 정보에 의해 생성된 사용자 권한키를 상기 인증 서버로부터 입력받는 단계;

상기 사용자 권한키에 의해 상기 파일 암호화키에 상응하는 파일 복호화키를 생성하는 단계;

상기 생성된 파일 복호화키에 의해 상기 암호화된 디지털 컨텐츠 파일을 암호화하는 단계

를 포함하되,

상기 인증 서버는 상기 디지털 컨텐츠 제공 서버에 접속된 사용자의 정보 및 상기 디지털 컨텐츠 제공 서버 정보의 암호화에 의해 상기 서비스 등록키를 생성함을 특징으로 하는 클라이언트에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 10.

제9항에 있어서,

상기 시스템 정보는 적어도 CPU의 종류, 개수 및 하드디스크의 페이지 사이즈 정보를 포함함을 특징으로 하는 클라이언트에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 11.

제9항에 있어서,

상기 사용자 권한키는 서비스 등록키를 일정의 암호화 알고리즘을 이용하여 생성된 파일 암호화 초기키 및 상기 인증 서버 랜덤값을 포함하되,

상기 파일 암호화 초기키는 상기 서비스 등록키를 미리 설정된 키값을 이용하여 암호화함에 따라 생성된 제1 파일 암호화키에 의해 상기 클라이언트의 사용자 정보 및 상기 디지털 컨텐츠 제공 서버 정보를 암호화하여 생성됨을 특징으로 하는 클라이언트에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 12.

제9항에 있어서,

상기 사용자 권한키에 의해 상기 파일 암호화키에 상응하는 파일 복호화키를 생성하는 단계는

상기 시스템 정보를 미리 설정된 제1 키값에 의해 암호화하여 제1 파일 복호화키를 생성하는 단계;

상기 사용자 권한키 중 상기 인증 서버 랜덤값을 제1 파일 복호화키에 의해 암호화하여 제2 파일 복호화키를 생성하는 단계;

상기 사용자 권한키 중 상기 암호화된 파일 암호화 초기키를 상기 제2 파일 복호화키에 의해 복호화하여 파일 암호화 초기키를 생성하는 단계;

상기 인증 서버 랜덤값을 미리 설정된 제2 키값을 이용하여 암호화함에 따라 제3 파일 복호화키를 생성하는 단계;

상기 제3 파일 복호화키에 의해 상기 파일 암호화 초기키, 상기 디지털 컨텐츠 파일 ID 및 상기 인증 서버 랜덤값을 암호화하여 상기 파일 암호화키에 상응하는 파일 복호화키를 생성하는 단계

를 포함하는 클라이언트에 의한 디지털 컨텐츠 복제 방지 방법.

청구항 13.

네트워크를 통해 디지털 컨텐츠 제공 서버에 접속되는 인증 서버에 의한 디지털 컨텐츠 파일의 복제 방지 장치 -상기 디지털 컨텐츠 제공 서버는 암호화된 디지털 컨텐츠 파일을 클라이언트로 제공함 -에 있어서,

상기 클라이언트로부터의 사용자 정보에 따른 서비스 등록키를 생성하여 상기 디지털 컨텐츠 제공 서버로 전송하는 수단;

상기 클라이언트 단말기의 시스템 정보에 따른 사용자 권한키를 생성하여 상기 클라이언트로 전송하는 수단을 포함하되,

상기 디지털 컨텐츠 제공 서버는 상기 서비스 등록키를 다단계 암호화에 의한 파일 암호화키를 생성하여 상기 디지털 컨텐츠 파일을 암호화하고,

상기 클라이언트는 상기 사용자 권한키에 의한 다단계 암호화를 통해 상기 파일 암호화키에 상응하는 파일 복호화키를 생성하여 상기 암호화된 디지털 컨텐츠 파일을 복호화하는 것을 특징으로 하는 디지털 컨텐츠 복제 방지 장치.

청구항 14.

제13항에 있어서,

상기 클라이언트로부터의 사용자 정보에 따른 서비스 등록키를 생성하여 상기 디지털 컨텐츠 제공 서버로 전송하는 수단은

상기 클라이언트의 사용자 정보를 상기 디지털 컨텐츠 제공 서버를 통해 입력받는 수단;

상기 사용자 정보 및 상기 디지털 컨텐츠 제공 서버의 정보를 일정의 암호화 알고리즘에 의해 암호화하여 상기 서비스 등록키를 생성하는 수단;

상기 사용자 정보 및 상기 디지털 컨텐츠 제공 서버 정보와 상기 서비스 등록키를 저장하는 수단;

상기 서비스 등록키를 상기 디지털 컨텐츠 제공 서버로 전송하는 수단

을 포함하는 디지털 컨텐츠 복제 방지 장치.

청구항 15.

제14항에 있어서,

상기 사용자 정보는 상기 클라이언트의 주민등록번호 및 성명 정보를 포함하는 것을 특징으로 하는 디지털 컨텐츠 복제 방지 장치.

청구항 16.

제14항에 있어서,

상기 디지털 컨텐츠 제공 서버 정보는 상기 디지털 컨텐츠 제공 서버 번호 정보를 포함하는 것을 특징으로 하는 디지털 컨텐츠 복제 방지 장치.

청구항 17.

제14항에 있어서,

상기 암호화 알고리즘은 투피시(twofish) 알고리즘임을 특징으로 하는 디지털 컨텐츠 복제 방지 장치.

청구항 18.

제13항에 있어서,

상기 클라이언트 단말기의 시스템 정보에 따른 사용자 권한키를 생성하여 상기 클라이언트로 전송하는 수단은

상기 시스템 정보를 미리 설정된 키값에 의해 일정의 암호화 알고리즘을 적용하여 암호화함에 따른 제1 토큰키를 생성하는 수단;

상기 알고리즘을 사용하여 제1 토큰키에 의해 일정의 랜덤값을 암호화함에 따른 제2 토큰키를 생성하는 수단;

상기 알고리즘을 이용하여 상기 서비스 등록키를 암호화함에 의해 상기 디지털 컨텐츠 파일 암호화 초기키를 생성하는 수단;

상기 알고리즘을 이용하여 상기 생성된 파일 암호화 초기키를 상기 제2 토큰키에 의해 암호화하여 제3 토큰키를 생성하는 수단;

상기 제3 토큰키에 상기 랜덤값을 부가하여 사용자 권한키를 생성하는 수단;

상기 사용자 권한키를 상기 클라이언트로 전송하는 수단

을 포함하는 디지털 컨텐츠 복제 방지 장치.

청구항 19.

제18항에 있어서,

상기 시스템 정보는 적어도 CPU의 종류, 개수 및 하드디스크의 페이지 사이즈 정보를 포함하는 것을 특징으로 하는 디지털 컨텐츠 복제 방지 방법.

청구항 20.

제18항에 있어서,

상기 암호화 알고리즘은 투피시 알고리즘임을 특징으로 하는 디지털 컨텐츠 복제 방지 장치.

청구항 21.

네트워크를 통해 디지털 컨텐츠 제공 서버에 접속된 클라이언트에 의한 디지털 컨텐츠 파일의 복제 방지 장치 -상기 디지털 컨텐츠 제공 서버는 네트워크를 통해 접속된 인증 서버로부터 서비스 등록키를 제공받고, 상기 디지털 컨텐츠 제공 서버는 상기 서비스 등록키의 다단계 암호화에 의해 생성된 파일 암호화키를 이용하여 상기 디지털 컨텐츠 파일을 암호화함 -에 있어서,

상기 인증 서버로 상기 클라이언트 단말기의 시스템 정보를 전송하는 수단;

상기 시스템 정보에 의해 생성된 사용자 권한키를 상기 인증 서버로부터 입력받는 수단;

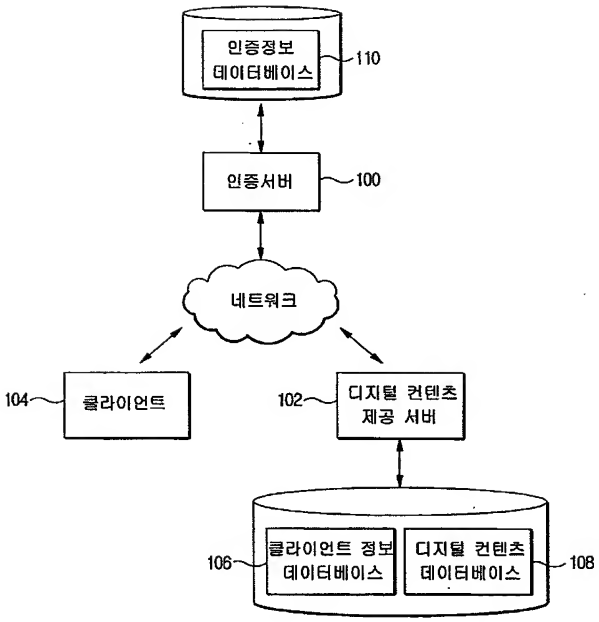
상기 사용자 권한키에 의해 상기 파일 암호화키에 상응하는 파일 복호화키를 생성하는 수단

을 포함하되,

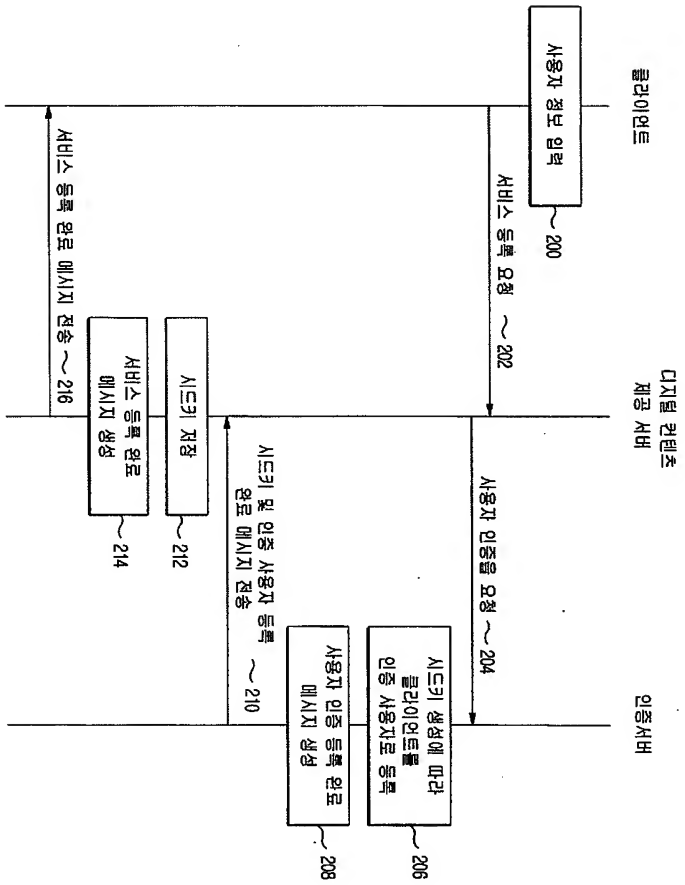
상기 인증 서버는 상기 디지털 컨텐츠 제공 서버에 접속된 사용자의 정보 및 상기 디지털 컨텐츠 제공 서버 정보의 암호화에 의해 상기 서비스 등록키를 생성함을 특징으로 하는 디지털 컨텐츠 복제 방지 장치.

도면

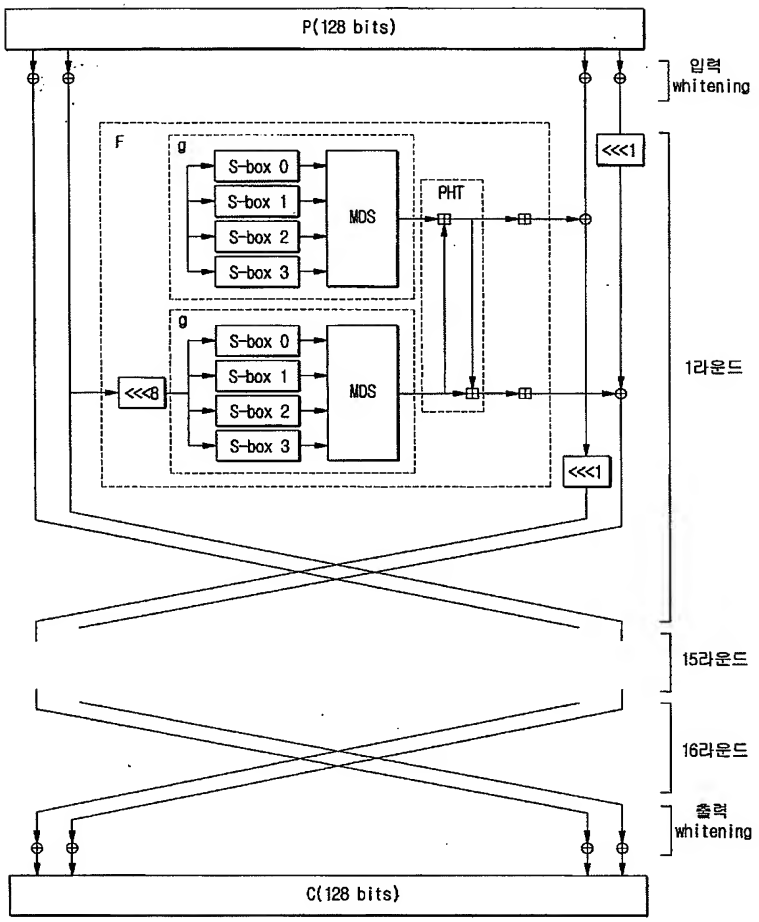
도면 1


인증정보
데이터베이스
110
인증서버
100
네트워크
104
클라이언트
102
디지털 컨텐츠
제공 서버
106
클라이언트 정보
데이터베이스
디지털 컨텐츠
데이터베이스
108

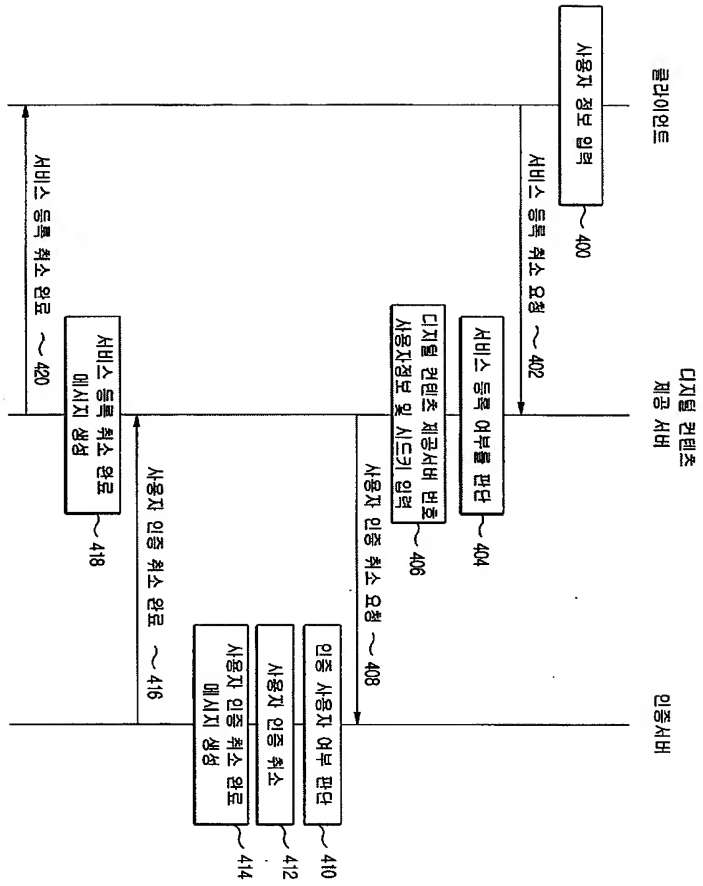
도면 2


클라이언트
디지털 컨텐츠 제공 서버
인증서버
사용자 정보 입력
~200
서비스 등록 요청 ~202
사용자 인증을 요청 ~204
시드키 생성에 따라 클라이언트를 인증 사용자로 등록
~206
사용자 인증 등록 완료 메시지 생성
~208
시드키 및 인증 사용자 등록 완료 메시지 전송 ~210
시드키 저장
~212
서비스 등록 완료 메시지 생성
~214
서비스 등록 완료 메시지 전송 ~216

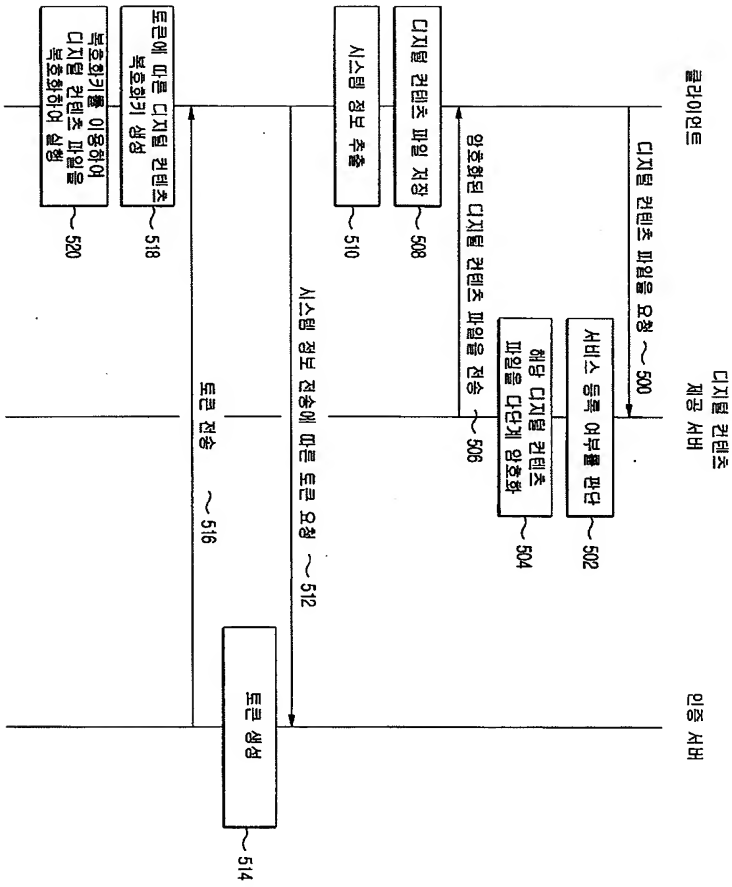
도면 3


P(128 bits)
입력 whitening
F
g
S-box 0
S-box 1
S-box 2
S-box 3
MDS
PHT
<<<1
<<<8
1라운드
15라운드
16라운드
출력 whitening
C(128 bits)

도면 4


클라이언트
디지털 컨텐츠 제공 서버
인증서버
사용자 정보 입력
400
서비스 등록 취소 요청
402
서비스 등록 여부를 판단
404
디지털 컨텐츠 제공서버 번호 사용자정보 및 시드키 입력
406
사용자 인증 취소 요청
408
인증 사용자 여부 판단
410
사용자 인증 취소
412
사용자 인증 취소 완료 메시지 생성
414
사용자 인증 취소 완료
416
서비스 등록 취소 메시지 생성
418
서비스 등록 취소 완료
420

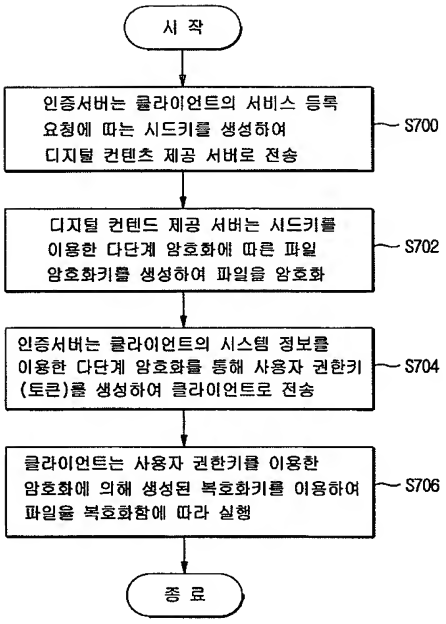
도면 5


클라이언트
디지털 컨텐츠 제공 서버
인증 서버
디지털 컨텐츠 파일을 요청 ~ 500
서비스 등록 여부를 판단 ~ 502
해당 디지털 컨텐츠 파일을 다단계 암호화 ~ 504
암호화된 디지털 컨텐츠 파일을 전송 ~ 506
디지털 컨텐츠 파일 저장 ~ 508
시스템 정보 추출 ~ 510
시스템 정보 전송에 따른 토큰 요청 ~ 512
토큰 생성 ~ 514
토큰 전송 ~ 516
토큰에 따른 디지털 컨텐츠 복호화키 생성 ~ 518
복호화키를 이용하여 디지털 컨텐츠 파일을 복호화하여 실행 ~ 520

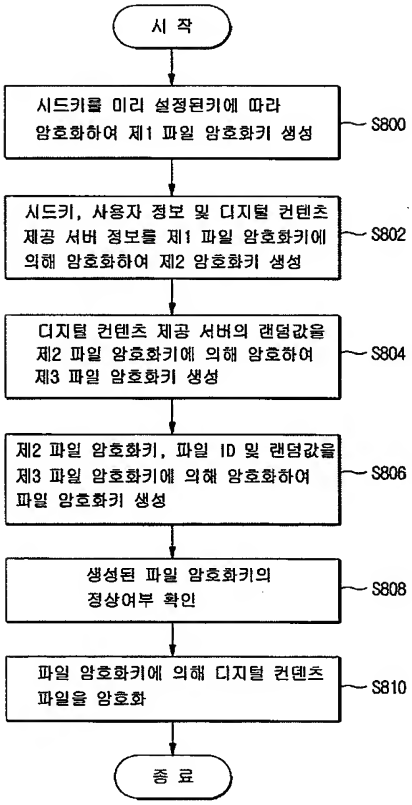
도면 6

	Index	구 분	bytes 수	내 용 (예시)
600	1	Magic Number	4	"Kr01":Korea #01, "cn01":China #01
602	2	Description	16	파일 설명
604	3	File Type	4	"0001":MP3, "0002":Print, "0003":
606	4	File ID	4	암호화 파일의 ID
608	5	User Name	16	사용자 이름
610	6	Flag	4	예비영역
612	7	Source Size	4	암호화할 파일의 총 사이즈
614	8	this Size	4	Header+Body+Extension의 총 사이즈
616	9	Body Size	4	암호화된 파일의 총 사이즈
618	10	Source Checksum	4	암호화할 파일의 Checksum
620	11	ICC Version	4	사용할수 있는 스마트카드의 버젼
622	12	Sp Server Random	16	서비스 서버의 랜덤
624	13	KVC	8	FKey가 정확한지 확인할 수 있는 Key 확인용 값
626	14	Reserved	28	RFU
628	15	Header Checksum	8	파일 헤더의 확인용 Checksum
	계		128	

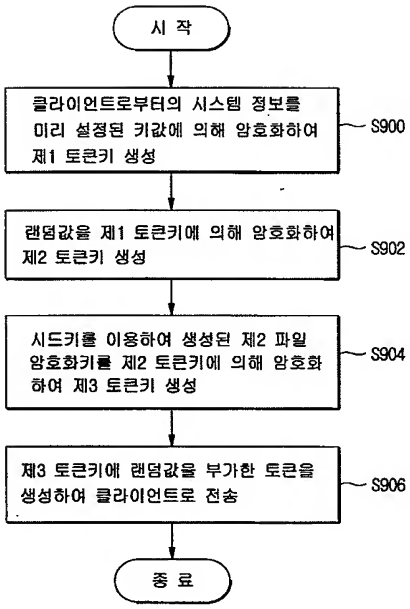
도면 7


시 작
인증서버는 클라이언트의 서비스 등록 요청에 따는 시드키를 생성하여 디지털 컨텐츠 제공 서버로 전송
S700
디지털 컨텐드 제공 서버는 시드키를 이용한 다단계 암호화에 따른 파일 암호화키를 생성하여 파일을 암호화
S702
인증서버는 클라이언트의 시스템 정보를 이용한 다단계 암호화를 통해 사용자 권한키 (토큰)를 생성하여 클라이언트로 전송
S704
클라이언트는 사용자 권한키를 이용한 암호화에 의해 생성된 복호화키를 이용하여 파일을 복호화함에 따라 실행
S706
종 료

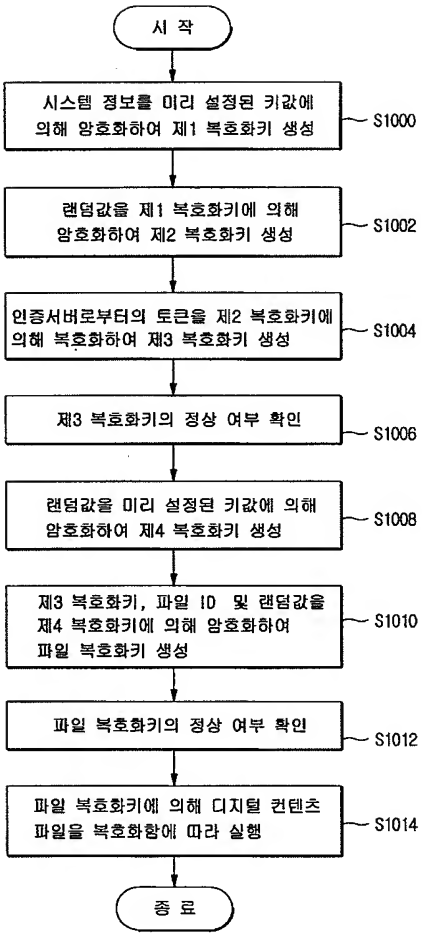
도면 8


시 작
시드키를 미리 설정된키에 따라 암호화하여 제1 파일 암호화키 생성
S800
시드키, 사용자 정보 및 디지털 컨텐츠 제공 서버 정보를 제1 파일 암호화키에 의해 암호화하여 제2 암호화키 생성
S802
디지털 컨텐츠 제공 서버의 랜덤값을 제2 파일 암호화키에 의해 암호하여 제3 파일 암호화키 생성
S804
제2 파일 암호화키, 파일 ID 및 랜덤값을 제3 파일 암호화키에 의해 암호화하여 파일 암호화키 생성
S806
생성된 파일 암호화키의 정상여부 확인
S808
파일 암호화키에 의해 디지털 컨텐츠 파일을 암호화
S810
종 료

도면 9


시 작
클라이언트로부터의 시스템 정보를 미리 설정된 키값에 의해 암호화하여 제1 토큰키 생성
S900
랜덤값을 제1 토큰키에 의해 암호화하여 제2 토큰키 생성
S902
시드키를 이용하여 생성된 제2 파일 암호화키를 제2 토큰키에 의해 암호화하여 제3 토큰키 생성
S904
제3 토큰키에 랜덤값을 부가한 토큰을 생성하여 클라이언트로 전송
S906
종 료

도면 10


시 작
시스템 정보를 미리 설정된 키값에 의해 암호화하여 제1 복호화키 생성
S1000
랜덤값을 제1 복호화키에 의해 암호화하여 제2 복호화키 생성
S1002
인증서버로부터의 토큰을 제2 복호화키에 의해 복호화하여 제3 복호화키 생성
S1004
제3 복호화키의 정상 여부 확인
S1006
랜덤값을 미리 설정된 키값에 의해 암호화하여 제4 복호화키 생성
S1008
제3 복호화키, 파일 ID 및 랜덤값을 제4 복호화키에 의해 암호화하여 파일 복호화키 생성
S1010
파일 복호화키의 정상 여부 확인
S1012
파일 복호화키에 의해 디지털 컨텐츠 파일을 복호화함에 따라 실행
S1014
종 료

(19) Korean Intellectual Property Office (KR)
(12) Patent Laid-Open Publication (A)

(51) Int. Cl.[7]
G06F 15/00

(11) Laid-Open Publication No.: 10-2002-0063659
(43) Laid-Open Publication Date: August 5, 2002

(21) Application No.: 10-2001-0004215
(22) Filing Date: January 30, 2001

(71) Applicant: Digicaps Co., Ltd.
Young-In Buld 3rd-4th Floors
Seocho-gu, Seocho 3 dong 1708-7, Seoul, Korea
(72) Inventors: Shin, Yong Tae
Hyundai Apt 20-1001
Apgujeong dong, Gangnam-gu, Seoul, Korea
(74) Attorney(s): Choi, Yie Wook

Request for examination: *Not filed*

(54) Apparatus and Method for Preventing Copy of Digital Contents

[Abstract]

The present invention relates to an apparatus and method for effective prevention of illegal copy of digital contents provided to clients. In the invention an authentication server generates a service subscription key based on user information from a client who accessed through a network and information about a digital content service server, and a user access key for decrypting a digital content file that is encrypted with system information of a client's terminal. The digital content service server generates a file encryption key through a multi-stage encryption of the service subscription key to encrypt a digital content file and provides it to a client. The client generates a file decryption key through the multi-stage encryption and decryption of the user access key to decrypt the encrypted digital content file. In addition, the present invention adopts the twofish algorithm for generating the service subscription key, the file encryption key and the file decryption key.

Representative Figure: Fig. 1

Key words
digital content, authentication server, copy, system information, file encryption key, file decryption key, twofish algorithm

Specification

Brief Description of Drawings

Fig. 1 is a schematic block diagram of an apparatus for preventing illegal copy of digital contents in accordance with the present invention.
Fig. 2 is a schematic view of the service subscription flow for a client.
Fig. 3 is a schematic view of a twofish block encryptor.
Fig. 4 is a schematic view of the service subscription cancellation for a client.
Fig. 5 is a schematic view of the digital content file receiving flow for a client.
Fig. 6 is a drawing showing a header configuration of an encrypted digital content file.
Fig. 7 is a flow chart for performing the digital content copy pretention in accordance with the present invention.
Fig. 8 is a flow chart for performing the generation of a file encryption key for digital content file encryption.
Fig. 9 is a flow chart for performing the generation of user access information with an authentication server.
Fig. 10 is a flow chart for performing the decryption of a digital content file in accordance with the present invention.

<Description of Reference Numerals for Main Parts of the Drawings>
100: authentication server
102: digital content service server
104: client
106: client information database
108: digital content information database
110: authentication information database

Detailed Description of the Invention
Objective(s) of the Invention

Technical Field of the Invention and Related art

The present invention relates to an apparatus and method for preventing illegal copy of digital contents, more specifically, to an apparatus and method for preventing illegal copy of digital contents to effectively prevent illegal copy of digital contents provided to clients.

The modernizers are flooded with information that comes through all kinds of media such as broadcasts, publications, and the like. There are now information providers who intend to integrate the information provided through all kinds of media and provide it at once, and there are users who want to selectively get only desired contents out of digital contents that are provided by the information providers.

Accordingly, there came digital content transmission systems composed of information providers who convert all kinds of information into digital contents and store the digital contents to provide them to individual users, and users who get digital contents from the information providers through a network.

Such a digital content transmission system provides users with an application program through which anyone can easily download digital contents.

In addition, a user who is accessed to such a digital content transmission system via a network can get all information he (she) desires through the downloaded application program.

Those digital contents from the digital content transmission systems are provided with or without charge to users.

Digital content transmission systems set service fee for a charged digital content.
When a user receives a digital content with service fee set therefor, a service server adds up service fees according to the user's information use volume and charges it to the user.

However, when users access to a system that provides digital contents commercially using a network and receive a digital content they should pay for, most of them give away the charged digital content as a crack to others without permission.

Besides, although damages on providers because of the use of copies of digital contents are serious, it is not possible to completely prevent them.

Technical Task to be Achieved by the Invention

Therefore, the present invention is devised to solve general problems of the related art, by providing an apparatus and method for preventing copy of digital contents to encrypt digital content files with a file encryption key that is generated through multi-encryption.

Also, another object of the present invention is to provide an apparatus and method for preventing copy of digital contents to generate a user access key used for decrypting an encrypted digital content file based on system information of a client terminal.

Construction and Operation of the Invention

To achieve the above described objects, an authentication server of the present invention generates a service subscription key based on user information from a client who accessed through a network and information about a digital content service server, and a user access key for decrypting a digital content file that is encrypted with system information of a client's terminal.

A digital content service server generates a file encryption key through a multi-stage encryption of the service subscription key to encrypt a digital content file and provides it to a client.

In addition, a client generates a file decryption key through the multi-stage encryption and decryption of the user access key to decrypt the encrypted digital content file.

Also, the present invention uses the twofish algorithm for generating the service subscription key, the file encryption key and the file decryption key.

Hereinafter, a preferred embodiment of an apparatus and method for preventing illegal copy of digital contents according to the present invention will be explained in detail.

Fig. 1 is a schematic block diagram of an apparatus for preventing illegal copy of digital contents in accordance with the present invention, Fig. 2 is a schematic view of the service subscription flow for a client, and Fig. 3 is a schematic view of a twofish block encryptor.

Fig. 4 is a schematic view of the service subscription cancellation for a client, Fig. 5 is a schematic view of the digital content file receiving flow for a client, and Fig. 6 is a drawing showing a header configuration of an encrypted digital content file.

As shown in Fig. 1, the present invention is configured by including an authentication server (100), a digital content service server (102), a client (104), a client information database (106), a digital content information database (108) and an authentication information database (110).

Here, the authentication server (100) is configured to generate a seed key (Cap ID) for encryption of a digital content file provided through the digital content service server (102) and for generation of file use access information for the client (104).

Here, the seed key (Cap ID) is a service subscription key for receiving digital content information, or receiving service to decrypt an encrypted digital content.

Also, for decryption of an encrypted digital content file, the authentication server (100) is configured to encrypt the seed key (Cap ID) and system information of the client (104) by a predetermined encryption algorithm, thereby generating a digital content file use access key (hereinafter, referred to as a token), and to transmit the generated token to the client (104).

Here, the system information of the client (104) for token generation is composed of CPU size, count number and page size information of hard disks and so on. Moreover, the encryption algorithm adopted for token generation is the twofish algorithm.

The digital content service server (102) is configured to generate a file encryption key (FKey1) through four-stage encryption of the seed key (Cap ID) that is transmitted from the authentication server (100) using the twofish algorithm.

The client (104) is configured to store the transmitted token from the authentication server (100) in a registry which is a storage region inside a terminal and to decrypt an encrypted digital content file by generating a file decryption key (FKey2) corresponding to the file encryption key (FKey1) through encryption and decryption in accordance with the token and the encrypted digital content file header information that is downloaded from the digital content service server (102).

Here, the present invention uses the twofish algorithm for key-encryption/decryption during the generation of the file encryption key (FKey1).

The client information database (106) is configured to store user information of the client (104) and a corresponding seed key (Cap ID), and the digital content information database (108) is configured to store digital content information that is classified depending on the file ID.

Furthermore, the authentication information database (110) is configured to store a relevant service subscription key of the client (104), that is, seed key (Cap ID).

Operations of the thusly configured digital content copy prevention apparatus according to the present invention are now explained as follows, with reference to accompanied drawings.

First, service subscription procedure of the client (104) for receiving a digital content file from the digital content service server (102) is explained with reference to Fig. 2.

The client (104) downloads a digital content run program to run a digital content file that is

transmitted from the digital content service server (102) and installs the digital content run program by executing the downloaded run program.

At this time, it is obvious that not only can downloading of the digital content run program be executed as part of the service subscription procedure, but the program can be downloaded prior to the service subscription.

Here, the digital content run program includes an MP3 player, a media player, or a real player, etc.

Next, the client (104) accesses to the digital content service server (102) through internet connection, for example, a network, inputs user information (S200) and requests service subscription (S202).

Here, user information includes at least name of the client (104), ID, password and resident registration number.

The digital content service server (102) stores, in the client information database (106), the user information inputted from the client (104), and requests authentication user registration by transmitting the resident registration number, the client's name (or ID) or the password and a digital content service server number (SP_NO) to the authentication server (100) (S204).

Here, the digital content service server number (SP_NO) is information for distinguishing in case there are plural digital content service servers networked to the authentication server (100).

The authentication server (100) generates a seed key (Cap ID) for authentication user registration requested from the digital content service server (102).

That is, the authentication server (100) performs encryption, as shown in Eq. 1, of the service providing server number (SP_NO), the resident registration number and the client's name that are transmitted from the digital content service server (102) with a first setup key (auLKey) in accordance with the twofish algorithm, and generates a seed key (Cap ID) (S206).

Here, a predetermined programmed key value may be set as the first setup key (auLKey).

Eq. 1

$$Cap\_ID = E_{auLKey}[SP\_NO(4) \,||\, \text{resident registration number (13)} \,||\, \text{client's name (30)}]$$

wherein, the numerals in round brackets stand for byte unit, the predetermined key value (auLKey) is a predetermined value given by a programmer for encryption, and E is the abbreviation for Encryption.

Here, the twofish algorithm is an algorithm adopted from ASE (Advanced Encryption Standard) published by NIST under United States Department of Commerce for replacement of data encryption standards.

The twofish algorithm is a 128-bit symmetrical block encryptor, has a variety of key lengths such as 128 bits, 192 bits, 256 bits and the like, and is efficient for diverse software and hardware platforms.

In addition, a twofish block encryptor as shown in Fig. 3 has a 16-round feistel network configuration along with a bijective function f, and includes an additional whitening section at its input/output unit.

Here, the feistel network is configured by including plural S–boxes, MDS matrix and PHT.

A cipher text generation procedure by the twofish block encryptor with the above-described configuration is now explained roughly.

An original text consists of 4r 32-bit words and performs a XOR operation with these four key words in the input whitening step. Later, 16 rounds are performed sequentially, and in each round two keys on the left side are used as an input for the function g, the most crucial part of the twofish.

The function g is composed of four byte wide keys and four key independent S-boxes, and a linear mixing step based on the MDS matrix is carried out. Results of the two functions g are combined using PHT, and two key words are added.

These two results become an XOR to be a XOR with words on the right side (first, one of them rotates to the left by 1 bit, and the other rotates later to the right).

Next, for the next processing phase half of the left side and half of the right side are changed, and in the final processing phase at the end of all processing phases the change becomes opposite.

And, four words are subject to the XOR with more than four words to generate a cipher text.
The authentication server (100) generates a user authentication registration complete message (S208) and transmits, to the digital content service server (102), a seed key (Cap ID) generated by the twofish algorithm that performs the operations described above and the message (S210).

The digital content service server (102) stores the seed key (Cap ID) from the authentication server (100) in the client information database (106) (S212), generates a service subscription complete message (S214) and transmits it to the client (104) (S216) .

Next, the process in response to a service subscription cancellation request from the client (104) is explained, with reference to Fig. 4.

First, the client (104) inputs user information, namely, resident registration number and password (S400) and transmits a service subscription request signal to the digital content service server (102) (S402).

The digital content service server (102) compares the resident registration number and password from the client (104) with client information stored in the client information database (106) to decide if the client (104) is a service subscriber (S404).

If the client (104) is a service subscriber, the digital content service server (102) searches a seed key (Cap ID) of the client (104), and transmits the digital content service server number (SP_NO), the resident registration number and the seed key (Cap ID) to the authentication server (100), thereby requesting (S408) the cancellation of user authentication (S406).

The authentication server (100) searches the authentication information database (110) in accordance with a user authentication cancellation request signal from the digital content service server (102) and decides if the client (104) is an authenticated user (S410).

If the client (104) is an authenticated user, the authentication server(100) deletes user authentication information of the client (104) to thus cancel user authentication (S412), and transmits the

generated user authentication cancellation complete message to the digital content service server (102) (S414).

The digital content service server (102) generates a service subscription cancellation complete message according to the user authentication cancellation complete message from the authentication server (100) (S418), and transmits the generated service subscription cancellation complete message to the client (104) to complete the cancellation of service subscription of the client (104) (S420).

Next, the process of how the client (104) having completed service subscription receives and executes a digital content file from the digital content service server (102) is explained, with reference to Fig. 5.

First, the client (104) accesses the digital content service server (102) through the network and logs on by inputting ID and password. Then, the client (104) inputs a file request signal for selecting one of a variety of digital content files being provided (S500).

The digital content service server (102) compares the ID and the password inputted by the client (104) with the relevant information stored in the client information database (106) to decide if the service subscription should be done (S502).

If the client (104) is a service subscriber, the digital content service server (102) generates a file key (FKey1) for encrypting a corresponding digital content file requested by the client (104) (S504).

That is, the digital content service server (102) performs the multi-stage encryption for the seed key (Cap ID) and the user information of the client using the twofish algorithm to generate a file encryption key (FKey1), and it will be explained in detail hereinafter.
First, the digital content service server (102) encrypts the seed key (Cap ID) of the client (104) that is stored in the client information database (106) using a second setup key (asUkey) to generate a first file encryption key (DasUKey1).

At this time, the second setup key (asUkey) may be composed identically with or differently from the first setup key (auLKey) given during the generation of the seed key (Cap ID).

Next, the digital content service server (102) generates, as shown in Eq. 2, a second file encryption key (UKey1) which is an initial encryption key for generating the file encryption key (FKey1), by encrypting the digital content service server number (SP_NO), the resident registration number and the stream of the seed key (Cap ID) in use of the first file encryption key (DasUKey1).

Eq. 2

$$UKey1 = E_{DasUKey1}\,[SP\_NO(4) \,||\, \text{resident registration number (13)} \,||\, \text{Cap ID (16)}]$$

wherein, E stands for the abbreviation for encryption, and the twofish algorithm was adopted as an algorithm for encryption, and the numerals in round brackets stand for byte numbers.

Moreover, the digital content service server (102) encrypts a random value of the digital content service server (102) in accordance with a predetermined key value (auPKey) and generates a third file encryption key (DauFKey1).

Here, the random value of the digital content service server is selected at random by a certain program and consists of 16 bytes.

Next, the digital content service server (102) encrypts, as shown in Eq. 3, the second file encryption key (UKey1), a selected digital content file ID and the digital content service server's random value using the third file encryption key (DauFKey1) to generate a file encryption key (FKey1).

Eq. 3

$FKey1 = E_{DauFKey1}$ [UKey1 (16) || file_ID (8) || digital content service server random (8)]

wherein, the numerals in round brackets stand for byte numbers, the digital content service server random value is selected at random by a certain program, and E is the abbreviation for encryption.

The digital content service server (102) encrypts a digital content file that is requested by the client (104) using the file encryption key (FKey1) that is generated through the multi-stage encryption and transmits it to the client (104).

At this time, the digital content file that is encrypted and transmitted to the client (104) has a header with the configuration shown in Fig. 6.

Referring to Fig. 6, header information of the digital content file includes a digital content service server number field (600), a file description field (602), a file type field (604), a file ID field (606), a client (104) name field (608), a first preliminary flag field (610), a target encryption file's total size field (612), a digital content file's total size field (614) including header, body and extension flag, an encrypted file's total size field (616), a checksum field (618) of a target encryption file for error detection, a second preliminary flag field (620), a service server random field (622), a file encryption key verification value (KVC) field (624), a third preliminary flag field (626) and a checksum field (628) for error detection of the file header.

Here, the verification value (KVC) of the file encryption key verification value field (624) is generated by encrypting a 16-byte null with the previous file encryption key, and the digital content service server (102) verifies if the generated file encryption key (FKey1) is valid by comparing the file encryption key (FKey1) that has been generated for file encryption with the verification value (KVC).

The client (104) downloads a digital content file including a header with the above described configuration and performs decryption to run the digital content file.

That is, the client (104) extracts system information to generate a decryption key of the downloaded digital content file and transmits a token request signal including the extracted system information.

In addition, the system information is information about the system of a client who requested a token and contains kind of CPU, count number, hard disk's page size, etc.

The authentication server (100) encrypts, as shown in Eq. 4, the service providing server number, the resident registration number and the system information transmitted from the client (104) with the first setup key (auLKey) and generates a first token key (LKey1).

Eq. 4

$LKey1 = E_{auLKey}$ [system information (16)]

wherein, E is the abbreviation for encryption, and the twofish algorithm was adopted as an algorithm for encryption, and the numerals in round brackets stand for bytes.

The authentication server (100) encrypts a 16-byte random value of the authentication server (100) using the generated first token key (LKey1) and generates a second token key (SLKey1). At this time, the authentication server (100) verifies validity by comparing a verification value that is generated by encrypting a 16-byte null with a previous second token key with the generated second token key (SLKey1).

Here, the random value of the authentication server (100) is randomly selected in the authentication server (100) through a certain program.

The authentication server (100) encrypts a 16-byte second file encryption key (UKey1) that is generated with the seed key (Cap ID) of the client (104) using the second token key (SLKey1) and generates a third token key (EncUKey1).

Here, since the second file encryption key (UKey1) is generated through the same procedure by the digital content service server (102), no detailed explanation will be provided.

The authentication server (100) transmits, to the client (104), a token that is configured in form of [digital content encryption server random (16) || third token (16)], the addition of a 16-byte authentication server random value to the third token key (EncUKey1).

At this time, the token is downloaded and stored in a storage region of a terminal and may be configured to limit the number of downloads of the token.

The client (104) extracts system information of the terminal, encrypts the extracted system information with a predetermined key value (auLKey) and generates a first decryption key (LKey2).

Moreover, the client (104) encrypts a random value in the token with the first decryption key (LKey2) and generates a second decryption key (SLKey1).

Here, the first decryption key (LKey2) and the second decryption key (SLKey2) that are generated by the client (104) are the same as the first token key (LKey1) and the second token ken (SLKey1) that are generated by the authentication server (100), and their generation procedures are also identical with each other.

The client (104) decrypts a third token key (EncUKey1) with the second decryption key (SLKey2) and generates a third decryption key (UKey2). It is obvious that the third decryption key (UKey2) is the same key as the second file encryption key (UKey1).

Furthermore, the client (104) encrypts the service providing server random extracted from an encrypted digital content file header with the third setup key (auFKey) and generates a fourth file key (DauFKey).

At this time, the third setup key (auFKey) may be configured identically with or different from the first setup key (auLKey) or the second setup key (asUKey).

The client (104) generates, as shown in Eq. 3, a file decryption key (FKey2) by encrypting the file ID extracted from an encrypted digital content file, the digital content service server random, the third decryption key (UKey2) and the fourth file key (DauFKey).

At this time, the client (104) verifies validity by comparing a verification key value in the

downloaded digital content file header with the generated file decryption key (FKey2).

The client (104) uses the generated fine decryption key (FKey2) to decrypt an encrypted digital content file and runs the digital content file with a run program.

Here, it is obvious that the file decryption key (FKey2) is the same as the file encryption key (FKey1) this is for the digital content service server (102) to encrypt a digital content file.

The following now explains, with reference to Fig. 7, the performance procedure of the digital content copy prevention apparatus of the present invention with the above described structure.

Fig. 7 is a flow chart for performing the digital content copy pretention in accordance with the present invention.

First, the digital content service server (102) transmits, to the authentication server, a service subscription request signal in accordance with user information input, etc., from the client (104) who accessed through the network, and the authentication server (100) generates a seed key based on the user information and transmits it to the digital content service server (102) (S700).

The digital content service server (102) performs the multi-phase encryption of the seed key (Cap ID) to generate a file encryption key (FKey1) and encrypts a digital content file requested by the client (104) with the generated file encryption key (FKey1) (S702).

Next, the authentication server (100) transmits a user access key (token) which is generated through the multi-phase encryption of system information of the client (104) terminal to the client (104) (S704).

Here, the system information is specific information for the client (104) terminal, and the token that is generated based on the system information conveys particular features for each client terminal.

The client (104) uses the token to generate a file decryption key (FKey2) through encryption and decryption and decrypts an encrypted digital content file with the file decryption key (FKey2) (S706).

At this time, an algorithm for use in encryption and decryption for generating a seed key, a file encryption key, a token and a file decryption key is the twofish algorithm.

In addition, the decrypted digital content file runs by a proper run program that is installed in the client (104) terminal.

The following now explains, with reference to Fig. 8, the file encryption key generation procedure during the digital content copy prevention procedure according to the present invention with the above described configuration.

Fig. 8 is a flow chart for performing the generation of a file encryption key for digital content file encryption.

The digital content service server (102) encrypts a seed key from the authentication server (100) with a predetermined hard coded key value on the cord by a programmer for example to generate a first file encryption key (DasUKey1) (S800).

Next, it encrypts the seed key, resident registration number of the client (104) and the digital content service server number with the first encryption key (DasUKey1) and generates a second file encryption key (UKey1) (S802).

It generates a third file encryption key (DauFKey1) by encrypting random value of the digital content service server, which is selected at random by a certain program, with the second file encryption key(UKey1)(S804).

It also encrypts a digital content service server random value that is set at random by a certain program with the second file encryption key (UKey1) and generates a file encryption key (FKey1) (S806).

Next, it compares a file encryption key verification key value (KVC) that is obtained by encrypting a null function with a previous file encryption key with the file encryption key (FKey1) and verifies if the generated file encryption key (FKey1) is valid (S808).

It encrypts a digital content file with the file encryption key (FKey1) whose validity is verified and transmits it to the client (104) (S810).

Here, an algorithm for use in encryption for generating the first through third file encryption keys and the file encryption key is the twofish algorithm.

Moreover, the procedure for generating user access information, that is, token, of Fig. 7 is now explained in more detail with reference to accompanying drawings.

Fig. 9 is a flow chart for performing the generation of user access information with the authentication server.

First, the authentication server (100) encrypts system information from the client (104) with a predetermined key value (auLKey) to generate a first token key (LKey1) (S900), and encrypts a random value of the authentication server (100) with the generated first token key (LKey1) to generate a second token key (SLKey1) (S902).

Next, it encrypts the second file encryption key (UKey1) that is generated with the seed key (Cap ID) through the second token key (SLKey1) and generates a third token key (EncUKey1) (S904).

Here, since the second file encryption key (UKey1) is generated through the same procedure in Fig. 8, no detailed description will be provided.

The authentication server (100) generates a token in form of the addition of a 16-byte random value to the generated third token key (EncUKey1) and transmits it to the client (104) (S906).

The decryption procedure of a digital content file encrypted by the client is now explained in detail with reference to Fig. 10.

Fig. 10 is a flow chart for performing the decryption of a digital content file in accordance with the present invention.

The client (104) extracts system information of a terminal and encrypts the extracted system information with a predetermined key value (auLKey) to generate a first decryption key (LKey2) (S1000).

Next, it encrypts a random value among the tokens having been transmitted from the authentication server (100) and stored in a certain storage region of the terminal with the first decryption key (LKey2) and generates a second decryption key (SLKey2) (S1002).

It decrypts the third token key (EncUKey1) among the tokens with the second decryption key (SLKey2) to generate a third decryption key (UKey2) (S1004), and determines the validity of the third decryption key (UKey2) by comparing the generated third decryption key (UKey2) with a verification key value (KVC) (S1006).

Here, the verification key value (KVC) is a key value generated through the encryption of a null composed of only '0' bytes with the previous third decryption key (UKey2).

It encrypts a random value among the tokens with the third decryption key (UKey2) that is generated from the previous step (S1004) and generates a fourth decryption key (DauFKey2) (S1008).

Next, it encrypts the third decryption key (UKey2), the file ID, and the random value with the fourth decryption key (DauFKey2) to generate a file decryption key (FKey2) (S1010), and verifies validity of the file decryption key (FKey2) by comparing it with a verification key value (KVC) of a stored digital content file header (S1012).

It decrypts a digital content file that is encrypted with the valid file decryption key (FKey2) and runs the digital content file by a corresponding run program installed in the terminal (S1014).

Here, it is obvious that the third decryption key (UKey2) is identical with the second file encryption key (FKey1), and the file decryption key (FKey2) is identical wit the file encryption key (FKey1).

Effects of the Invention

The apparatus and method for preventing copy of digital contents according to the present invention generate, through the multi-stage encryption procedure, a file encryption key for encrypting digital contents, user access information for downloading a digital content file or for decrypting a downloaded digital content file and a file decryption key.

Therefore, according to the present invention, since the file encryption key, the user access information and the file decryption key are generated through the multi-stage encryption procedure, decoding those keys is almost impossible so copy of digital content files can be prevented.

In addition, since the user access information is generated with a key value contained in the system information of a terminal, the present invention can also be effective for prevention of copy of downloaded content files on the client terminal to another terminal.

(57) What is claimed is:

1. A method for preventing copy of digital content files by an authentication server accessed to a digital content service server through a network, with the digital content service server providing an encrypted digital content file to a client, comprising the steps of:

generating a service subscription key based on user information from the client and transmitting it to the digital content service server; and

generating a user access key based on system information of the client terminal and transmitting it to the client,

wherein the digital content service server generates a file encryption key through multi-stage encryption of the service subscription key to encrypt the digital content files, and

wherein the client generates a file decryption key corresponding to the file encryption key through the multi-stage encryption with the user access key and decrypts the encrypted digital content files.

2. The method of claim 1, wherein the step for generating a service subscription key based on user information from the client and transmitting it to the digital content service server comprises the steps of:

receiving user information of the client through the digital content service server;

encrypting the user information and information on the digital content service server through a predetermined encryption algorithm to generate the service subscription key;

storing the user information and the digital content service server and the service subscription key; and

transmitting the service subscription key to the digital content service server.

3. The method of claim 1 or claim 2, wherein the user information contains resident registration number and name information of the client.

4. The method of claim 2, wherein the information on the digital content service server contains number information of the digital content service server.

5. The method of claim 2, wherein the encryption algorithm is a twofish algorithm.

6. The method of claim 1, wherein the step for generating a user access key based on system information of the client terminal and transmitting it to the client comprises the steps of:

generating a user access key based on system information of the client terminal and transmitting it to the client;

generating a first token key through encryption of the system information by applying a predetermined encryption algorithm with a predetermined key value;

generating a second token key through encryption of a predetermined random value by adopting the algorithm with the first token key;

generating an encryption initial key of the digital content file through encryption of the service subscription key by adopting the algorithm;

generating a third token key through encryption of the generated file encryption initial key by adopting the algorithm with the second token key;

generating a user access key by adding the random value to the third token key; and

transmitting the user access key to the client.

7. The method of claim 6, wherein the system information contains at least kind of CPU, count number and page size information of a hard disk.

8. The method of claim 6, wherein the encryption algorithm is a twofish algorithm.

9. A method for preventing copy of digital contents by a client accessed to a digital content service server through a network, with the digital content service server receiving a service subscription key from a networked authentication server, with the digital content service server encrypting the digital content files using a file encryption key that is generated through multi-phase encryption of the service subscription key, comprising the steps of:

transmitting terminal system information of the client to the authentication server;

receiving, from the authentication server, a user access key generated based on the system information;

generating, with the user access key, a file decryption key corresponding to the file encryption key; and

encrypting the encrypted digital content file with the generated file decryption key,

wherein the authentication server generates the service subscription key through encryption of information on a user who is accessed to the digital content service server and through encryption of information on the digital content service server.

10. The method of claim 9, wherein the system information contains at least kind of CPU, count number and page size information of a hard disk.

11. The method of claim 9, wherein the user access key includes a file encryption initial key that is generated by encrypting the service subscription key with a predetermined encryption algorithm and the authentication server random value, with the file encryption initial key being generated by encrypting user information on the client and information on the digital content service server with a first file encryption key that is generated by encrypting the service subscription key with a predetermined key value.

12. The method of claim 9, generating a file decryption key corresponding to the file encryption key with the user access key comprises the steps of:

generating a first file decryption key by encrypting the system information with a predetermined first key value;

generating a second file decryption key by encrypting the authentication server random value among the user access keys with the first file decryption key;

generating a file encryption initial key by decrypting the encrypted file encryption initial key among the user access keys with the second file decryption key;

generating a third file decryption key by encrypting the authentication server random value with a predetermined second key value; and

generating a file decryption key corresponding to the file encryption key by encrypting, with the third file decryption key, the file encryption initial key, the digital content file ID, and the authentication server random value.

13. An apparatus for preventing copy of digital content files by an authentication server accessed to a digital content service server through a network, with the digital content service server providing an encrypted digital content file to a client, comprising:

a means for generating a service subscription key based on user information from the client and transmitting it to the digital content service server; and

a means for generating a user access key based on system information of the client terminal and transmitting it to the client,

wherein the digital content service server generates a file encryption key through multi-stage encryption of the service subscription key to encrypt the digital content files, and

wherein the client generates a file decryption key corresponding to the file encryption key through the multi-stage encryption with the user access key and decrypts the encrypted digital content files.

14. The apparatus of claim 13, wherein the means for generating a service subscription key based on user information from the client and transmitting it to the digital content service server comprises:

a means for receiving user information of the client through the digital content service server;

a means for encrypting the user information and information on the digital content service server through a predetermined encryption algorithm to generate the service subscription key;

a means for storing the user information and the digital content service server and the service subscription key; and

a means for transmitting the service subscription key to the digital content service server.

15. The apparatus of claim 14, wherein the user information contains resident registration number and name information of the client.

16. The apparatus of claim 14, wherein the information on the digital content service server contains number information of the digital content service server.

17. The apparatus of claim 14, wherein the encryption algorithm is a twofish algorithm.

18. The apparatus of claim 13, wherein the means for generating a user access key based on system information of the client terminal and transmitting it to the client comprises:

a means for generating a user access key based on system information of the client terminal and transmitting it to the client;

a means for generating a first token key through encryption of the system information by applying a predetermined encryption algorithm with a predetermined key value;

a means for generating a second token key through encryption of a predetermined random value by adopting the algorithm with the first token key;

a means for generating an encryption initial key of the digital content file through encryption of the service subscription key by adopting the algorithm;

a means for generating a third token key through encryption of the generated file encryption initial key by adopting the algorithm with the second token key;

a means for generating a user access key by adding the random value to the third token key; and

a means for transmitting the user access key to the client.

19. The apparatus of claim 18, wherein the system information contains at least kind of CPU, count number and page size information of a hard disk.

20. The apparatus of claim 18, wherein the encryption algorithm is a twofish algorithm.

21. An apparatus for preventing copy of digital contents by a client accessed to a digital content service server through a network, with the digital content service server receiving a service subscription key from a networked authentication server, with the digital content service server encrypting the digital content files using a file encryption key that is generated through multi-phase encryption of the service subscription key, comprising:

a means for transmitting terminal system information of the client to the authentication server;

a means for receiving, from the authentication server, a user access key generated based on the system information; and

a means for generating, with the user access key, a file decryption key corresponding to the file encryption key;

wherein the authentication server generates the service subscription key through encryption of information on a user who is accessed to the digital content service server and through encryption of information on the digital content service server.

Description of Drawings

Fig. 1

인증 정보 데이터베이스 110: Authentication information database
인증서버 100: Authentication server
네트워크: Network
클라이언트 104: Client
디지털 컨텐츠 제공 서버 102: Digital content service server
클라이언트 정보 데이터베이스 106: Client information database
디지털 컨텐츠 데이터베이스 108: Digital content database

Fig. 2

클라이언트: Client
디지털 컨텐츠 제공 서버: Digital content service server
인증서버: Authentication server
사용자 정보 입력 200 : Input user information
서비스 등록 요청 202: Request service subscription
사용자 인증을 요청 204: Request user authentication
시드키 생성에 따라 클라이언트를 인증 사용자로 등록 206: Register client as authorized user according to seed key generation
사용자 인증 등록 완료 메시지 생성 208: Generate user authentication subscription complete message
시드키 및 인증 사용자 등록 완료 메시지 전송 210: Transmit the seed key and the authenticated user registration complete message
시드키 저장 212: Storing the seed key
서비스 등록 완료 메시지 생성 214: Generate service subscription complete message
서비스 등록 완료 메시지 전송 216: Transmit the service subscription complete message

Fig. 3

입력 whitening: Input whitening
1 라운드: 1st round
15 라운드: 15th round
16 라운드: 16th round
출력 whitening: Output whitening

Fig. 4

클라이언트: Client
디지털 컨텐츠 제공 서버: Digital content service server
인증서버: Authentication server
사용자 정보 입력 400: User information input
서비스 등록 취소 요청 402: Service subscription cancellation request
서비스 등록 여부를 판단 404: Decision on service subscription
디지털 컨텐츠 제공 서버 번호 사용자 정보 및 시드키 입력 406: Digital content service server number, user information and seed key input
사용자 인증 취소 요청 408: User authentication cancellation request
인증 사용자 여부 판단 410: Decision on authenticated user
사용자 인증 취소 412: User authentication cancellation
사용자 인증 취소 완료 메시지 생성 414: Generating user authentication cancellation complete message
사용자 인증 취소 완료 416: Completing user authentication cancellation

서비스 등록 취소 완료 메시지 생성 418: Generating service subscription cancellation complete message
서비스 등록 취소 완료 420: Completing service subscription cancellation

Fig. 5

클라이언트: Client
디지털 컨텐츠 제공 서버: Digital content service server
인증서버: Authentication server
디지털 컨텐츠 파일 요청 500: Request digital content file
서비스 등록 여부를 판단 502: Decision on service subscription
해당 디지털 컨텐츠 파일을 다단계 암호화 504:
Multi-phase encryption of related digital content file
암호화된 디지털 컨텐츠 파일을 전송 506: Transmit encrypted digital content file
디지털 컨텐츠 파일 저장 508: Store digital content file
시스템 정보 추출 510: Extract system information
시스템 정보 전송에 따른 토큰 요청 512:
Request token following the transmission of system information
토큰 생성 514: Token generation
토큰 전송 516: Token transmission
토큰에 따른 디지털 컨텐츠 복호화키 생성 518:
Generate digital content decryption key according to token
복호화키를 이용하여 디지털 컨텐츠 파일을 복호화하여 실행 520:
Decrypt digital content file with decryption key and run the file

Fig. 6

구분: Division
byte 수: byte numbers
내용 (예시): Content (example)
파일 설명: File description
암호화 파일의 ID: Target encryption file ID
사용자 이름: User name
예비 영역: Preliminary flag
암호화할 파일의 총 사이즈: Total size of target encryption file
Header+Body+Extension 의 총사이즈: Total size of Header+Body+Extension
암호화된 파일의 총 사이즈: Total size of encrypted file
암호화할 파일의 Checksum: Checksum of target encryption file
사용할 수 있는 스마트 카드의 버전: Version of available smart card
서비스 서버의 랜덤: Random of service server
FKey 가 정확한지 확인할 수 있는 Key 확인용 값:
Key verification value to verify validity of FKey
파일 헤더의 확인용 Checksum: Verification checksum of file header
계: Total

Fig. 7

시작: Start

인증 서버는 클라이언트의 서비스 등록 요청에 따른 시드키를 생성하여 디지털 컨텐츠 제공 서버로 전송 S700:
Authentication server generates seed key at the request of client's service subscription and transmits to digital content service server.

디지털 컨텐츠 제공 서버는 시드키를 이용한 다단계 암호화에 따른 파일 암호화키를 생성하여 파일을 암호화 S702:

Digital content service server generates file encryption key through multi-stage encryption with the seed key to encrypt file.

인증서버는 클라이언트의 시스템 정보를 이용한 다단계 암호화를 통해 사용자 권한키(토큰)를 생성하여 클라이언트로 전송 S704:

Authentication server generates user access key through multi-stage encryption with client's system information and transmits to client.

클라이언트는 사용자 권한키를 이용한 암호화에 의해 생성된 복호화키를 이용하여 파일을 복호화함에 따라 실행 S706:
Client decrypts file with decryption key generated through encryption with the user access key and runs the file.

종료: End

Fig. 8

시작: Start

시드키를 미리 설정된키에 따라 암호화하여 제 1 파일 암호화키 생성 S800:
Generate 1st file encryption key by encrypting seed key with predetermined key

시드키, 사용자 정보 및 디지털 컨텐츠 제공 서버 정보를 제 1 파일 암호화키에 의해 암호화하여 제 2 암호화키 생성 S802:
Generate 2nd encryption key by encrypting seed key, user information and information of digital content service server with the 1st file encryption key

디지털 컨텐츠 제공 서버의 랜덤값을 제 2 파일 암호화키에 의해 암호화여 제 3 파일 암호화키 생성 S804:
Generate 3rd file encryption key by encrypting random value of digital content service server with the 2nd file encryption key

제 2 파일 암호화키, 파일 ID ac 랜덤값을 제 3 파일 암호화키에 의해 암호화아여 파일 암호화키 생성 S806:
Generate file encryption key by encrypting 2nd file encryption key, file ID and random value with the 3rd file encryption key

생성된 파일 암호화키의 정상 여부 확인 S808:
Verify validity of the generated file encryption key

파일 암호화키에 의해 디지털 컨덴츠 파일을 암호화 S810:
Encrypt digital content file with the file encryption key

종료: End

Fig. 9

시작: Start

클라이언트로부터의 시스템 정보를 미리 설정된 키값에 의해 암호화하여 제 1 토큰키 생성 S900:
Generate 1st token key by encrypting system information from client with predetermined key value

랜덤값을 제 1 토큰키에 의해 암호화하여 제 2 토큰키 생성 S902:
Generate 2nd token key by encrypting random value with 1st token key

시드키를 이용하여 생성된 제 2 파일 암호화키를 제 2 토큰키에 의해 암호화하여 제 3 토큰키를 생성 S904:
Generate 3rd token key by encrypting 2nd file encryption key in use seed key with the 2nd token key

제 3 토큰키에 랜덤값을 부가한 토큰을 생성하여 클라이언트로 전송 S906:
Generate token by adding random value to the 3rd token key and transmitting to client

종료: End

Fig. 10

시작: Start

시스템 정보를 미리 설정된 키값에 의해 암호화하여 제 1 복호화키 생성 S1000:
Encrypt system information with predetermined key value and generate 1st decryption key

랜덤값을 제 1 복호화키에 의해 암호화하여 제 2 복호화키 생성 S1002:
Generate 2nd decryption key by encrypting random value with the 1st decryption key

인증서버로부터 토큰을 제 2 복호화키에 의해 복호화하여 제 3 복호화키 생성 S1004:
Generate 3rd decryption key by decrypting token from authentication server with the 2nd decryption key

제 3 복호화키의 정상 여부 확인 S1006:
Verify validity of the 3rd decryption key

랜덤값을 미리 설정된 키값에 의해 암호화하여 제 4 복호화키 생성 S1008:
Generate 4th decryption key by encrypting random value with predetermined key value

제 3 복호화키, 파일 ID 및 랜덤값을 제 4 복호화키에 의해 암호화하여 파일 복호화키 생성 S1010:
Generate file decryption key by encrypting the 3rd decryption key, file ID and random value with the 4th decryption key

파일 복호화키의 정상 여부 확인 S1012:
Verify validity of file the file decryption key

파일 복호화키에 의해 디지털 컨텐츠 파일을 복호화함에 따라 실행 S1014:
Decrypt digital content file with the file decryption key and run the file

종료: End

FIG. 1

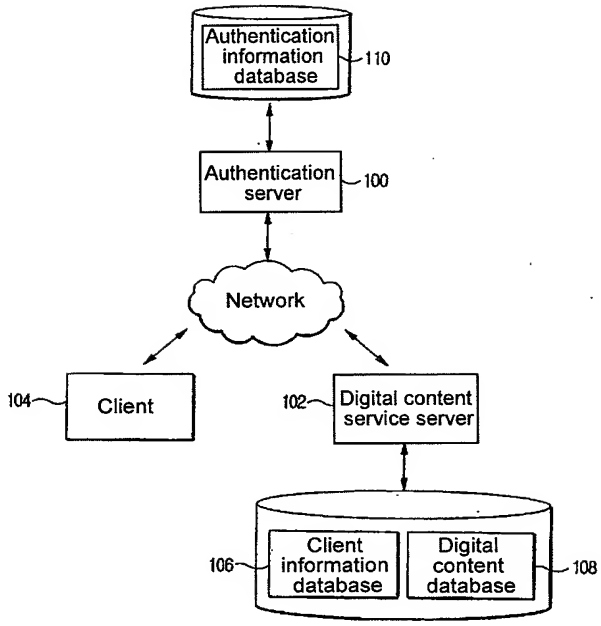

Authentication information database
110
Authentication server
100
Network
104
Client
102
Digital content service server
106
Client information database
Digital content database
108

FIG. 2

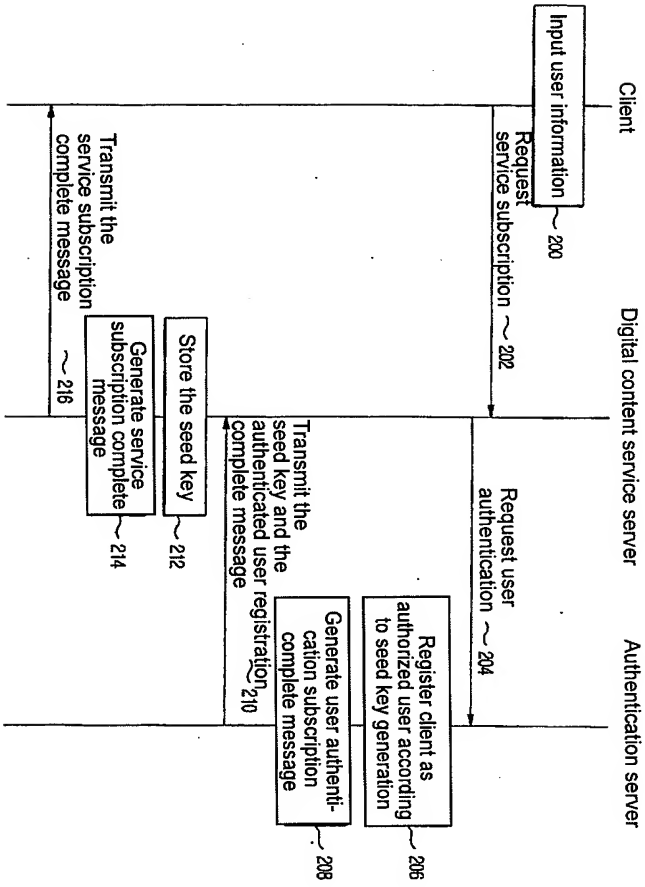

Client
Digital content service server
Authentication server
Input user information
200
Request service subscription
202
Request user authentication
204
Register client as authorized user according to seed key generation
206
Generate user authentication complete message
208
Transmit the seed key and the authenticated user registration complete message
210
Store the seed key
212
Generate service subscription complete message
214
Transmit the service subscription complete message
216

FIG. 3

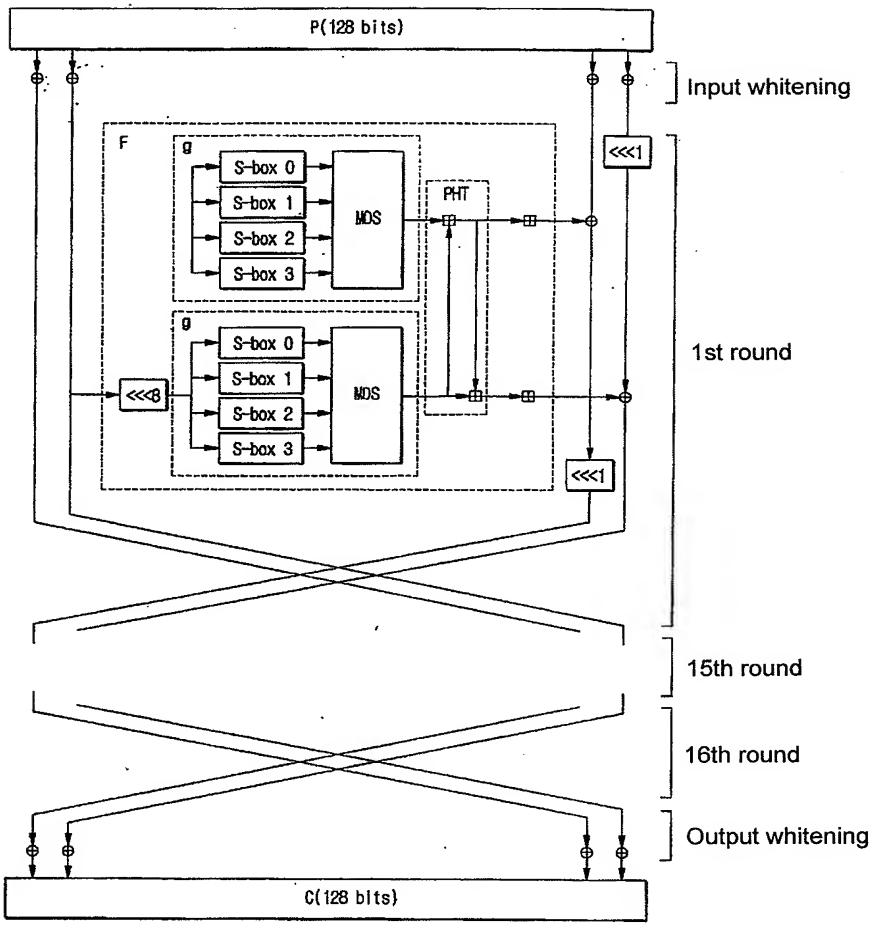

P(128 bits)
Input whitening
F
g
S-box 0
S-box 1
S-box 2
S-box 3
MDS
PHT
<<<1
g
S-box 0
S-box 1
S-box 2
S-box 3
MDS
<<<8
<<<1
1st round
15th round
16th round
Output whitening
C(128 bits)

FIG. 4

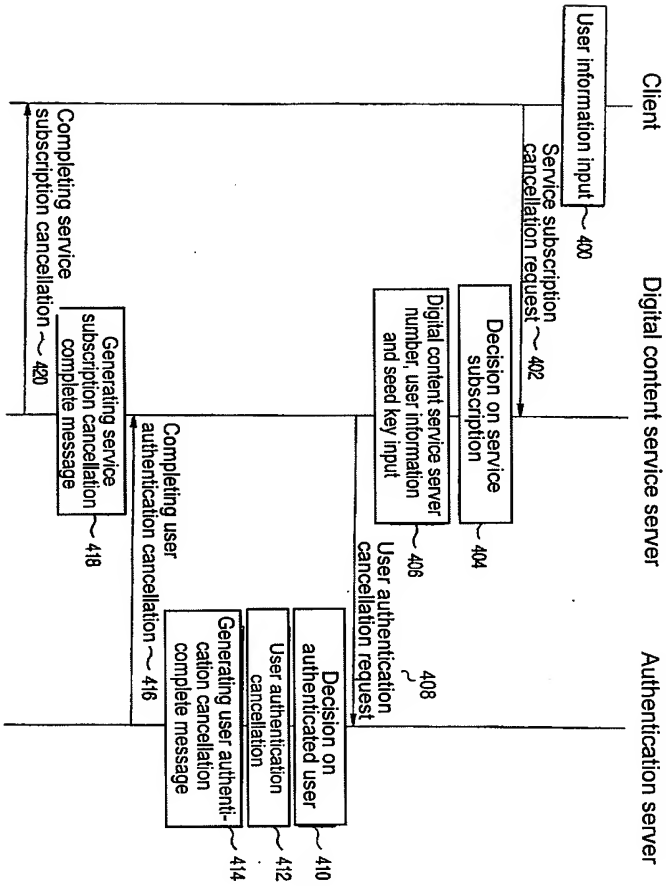

Client
Digital content service server
Authentication server
User information input
400
Service subscription cancellation request
402
Decision on service subscription
404
Digital content service server number, user information and seed key input
406
User authentication cancellation request
408
Decision on authenticated user
410
User authentication cancellation
412
Generating user authentication cancellation complete message
414
Completing user authentication cancellation
416
Generating service subscription cancellation complete message
418
Completing service subscription cancellation
420

FIG. 5

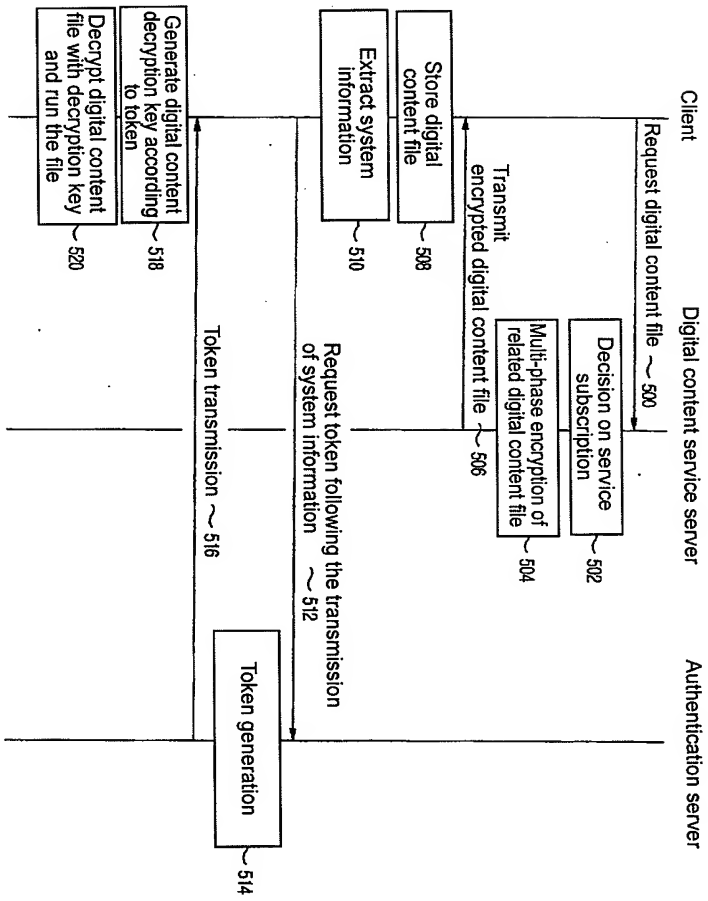

Client
Digital content service server
Authentication server
Request digital content file
500
Decision on service subscription
502
Multi-phase encryption of related digital content file
504
Transmit encrypted digital content file
506
Store digital content file
508
Extract system information
510
Request token following the transmission of system information
512
Token generation
514
Token transmission
516
Generate digital content decryption key according to token
518
Decrypt digital content file with decryption key and run the file
520

FIG. 6

	Index	Division	byte numbers	Content (example)
600	1	Magic Number	4	"Kr01":Korea #01, "cn01":China #01
602	2	Description	16	File description
604	3	File Type	4	"0001":MP3, "0002":Print, "0003":
606	4	File ID	4	Target encryption file ID
608	5	User Name	16	User name
610	6	Flag	4	Preliminary flag
612	7	Source Size	4	Total size of target encryption file
614	8	this Size	4	Total size of Header+Body+Extension
616	9	Body Size	4	Total size of encrypted file
618	10	Source Checksum	4	Checksum of target encryption file
620	11	ICC Version	4	Version of available smart card
622	12	Sp Server Random	16	Random of service server
624	13	KVC	8	Key verification value to verify validity of FKey
626	14	Reserved	28	RFU
628	15	Header Checksum	8	Verification checksum of file header
	Total		128	

FIG. 7

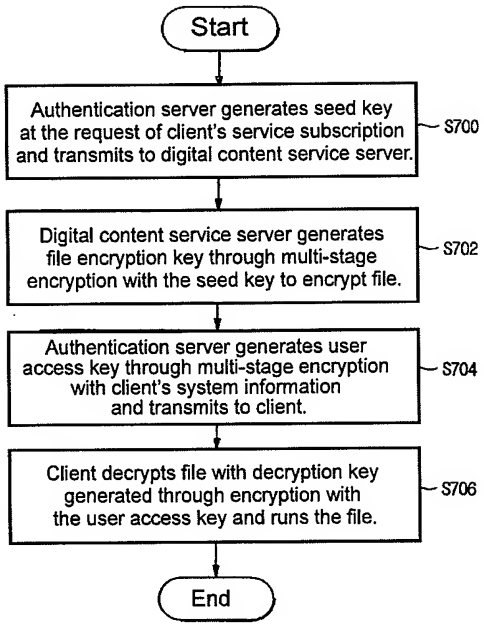

Start
Authentication server generates seed key at the request of client's service subscription and transmits to digital content service server.
S700
Digital content service server generates file encryption key through multi-stage encryption with the seed key to encrypt file.
S702
Authentication server generates user access key through multi-stage encryption with client's system information and transmits to client.
S704
Client decrypts file with decryption key generated through encryption with the user access key and runs the file.
S706
End

FIG. 8

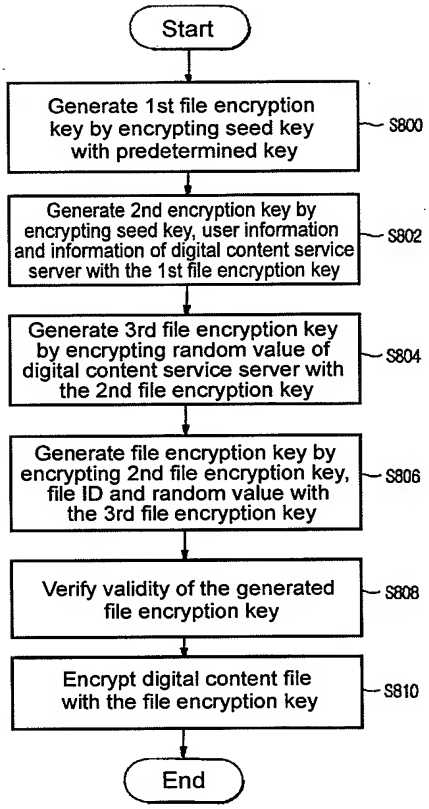

Start
Generate 1st file encryption key by encrypting seed key with predetermined key
S800
Generate 2nd encryption key by encrypting seed key, user information and information of digital content service server with the 1st file encryption key
S802
Generate 3rd file encryption key by encrypting random value of digital content service server with the 2nd file encryption key
S804
Generate file encryption key by encrypting 2nd file encryption key, file ID and random value with the 3rd file encryption key
S806
Verify validity of the generated file encryption key
S808
Encrypt digital content file with the file encryption key
S810
End

FIG. 9

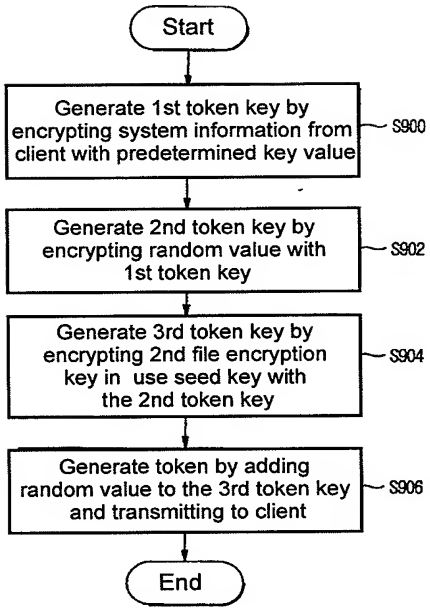
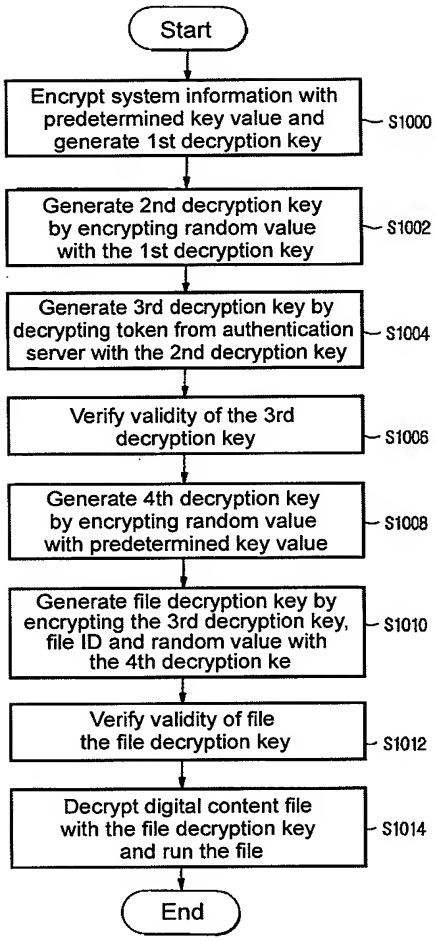

Start
Generate 1st token key by encrypting system information from client with predetermined key value
S900
Generate 2nd token key by encrypting random value with 1st token key
S902
Generate 3rd token key by encrypting 2nd file encryption key in use seed key with the 2nd token key
S904
Generate token by adding random value to the 3rd token key and transmitting to client
S906
End

FIG. 10


Start
Encrypt system information with predetermined key value and generate 1st decryption key
S1000
Generate 2nd decryption key by encrypting random value with the 1st decryption key
S1002
Generate 3rd decryption key by decrypting token from authentication server with the 2nd decryption key
S1004
Verify validity of the 3rd decryption key
S1006
Generate 4th decryption key by encrypting random value with predetermined key value
S1008
Generate file decryption key by encrypting the 3rd decryption key, file ID and random value with the 4th decryption ke
S1010
Verify validity of file the file decryption key
S1012
Decrypt digital content file with the file decryption key and run the file
S1014
End